Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и кибербезопасности
Высшая школа программной инженерии

Практическая работа №2

по дисциплине «Сети и телекоммуникации»

Выполнил: Яровой В. Д.
Группа: 5130904/00104

Проверил: Медведев Б. М.

Санкт-Петербург
2024

Содержание

1 Ответы на вопросы

1.1 Вопрос 1

TODO

Архитектура современной почтовый системы: Протоколы: SMTP, POP3, IMAP – зачем нужны MTA, MDA, MUA – что это Примеры используемого софта

Протоколы:

- SMTP (Simple Mail Transfer Protocol): Используется для отправки электронных писем. Отправитель передает письмо на почтовый сервер, который затем доставляет его получателю.
- POP3 (Post Office Protocol version 3): Используется для загрузки электронных писем с сервера на клиентское устройство (обычно почтовый клиент). Письма обычно удаляются с сервера после загрузки.
- IMAP (Internet Message Access Protocol): Также используется для доступа к электронным письмам на сервере, но письма остаются на сервере и синхронизируются между клиентским устройством и сервером.

Архитектурные компоненты:

- MTA (Mail Transfer Agent): Программное обеспечение, ответственное за передачу электронных писем между почтовыми серверами.
- MDA (Mail Delivery Agent): Программное обеспечение, отвечающее за доставку электронных писем на конечное устройство получателя или их хранение на сервере.
- MUA (Mail User Agent): Клиентское приложение, используемое конечным пользователем для чтения, отправки и управления электронными письмами

Примеры софта:

- MTA: Postfix, Exim, Sendmail.
- MDA: Dovecot, Cyrus.
- MUA: Microsoft Outlook, Mozilla Thunderbird, Apple Mail.

1.2 Вопрос 2

TODO

Типичный сценарий работы по протоколу SMTP

1. Отправитель устанавливает соединение с почтовым сервером получателя.
2. Отправляет команду HELO или EHLO для установки соединения.
3. Передает получателя командой MAIL FROM.
4. Указывает адрес получателя командой RCPT TO.
5. Отправляет само письмо с командой DATA.
6. Завершает передачу командой QUIT.

1.3 Вопрос 3

1.4 Вопрос 2

TODO

Коды ответов серверов SMTP/IMAP/POP3

SMTP (Simple Mail Transfer Protocol):

1. 2xx (успешно):
   - 211 – Система приняла команду. Информационный ответ.
   - 214 – Справочная информация по системе.
   - 220 – Сервер готов к работе.
   - 221 – Закрывается соединение.
   - 250 – Успешное выполнение команды.
2. 3xx (переадресация):
   - 354 – Ожидается ввод данных.
3. 4xx (временная недоступность):
   - 421 – Сервер временно недоступен.
   - 450 – Ошибка при передаче команды. Повторите.
4. 5xx (постоянная недоступность):
   - 501 – Синтаксическая ошибка в команде.
   - 550 – Невозможно выполнить команду.
   - 552 – Превышен лимит по размеру сообщения.

IMAP (Internet Message Access Protocol):

1. Основные:
   - OK: Команда выполнена успешно.
   - NO: Ошибка в выполнении команды.
   - BAD: Синтаксическая ошибка или неверный запрос.
2. Дополнительные:
   - PREAUTH: Сообщение перед успешной аутентификацией.
   - BYE: Закрывается соединение.

POP3 (Post Office Protocol version 3):

1. Основные:
   - +OK: Команда выполнена успешно.
   - -ERR: Ошибка в выполнении команды.
2. Дополнительные:
   - CAPA: Сервер поддерживает список возможностей.
   - TOP: Запрос заголовка и первых N строк сообщения.
   - USER/PASS: Аутентификация пользователя.
   - QUIT: Закрытие соединения.

1.5 Вопрос 4

TODO

В чем разница между протоколами **IMAP** и **POP3**

IMAP (Internet Message Access Protocol):
- Хранение: Сообщения хранятся на сервере.
- Синхронизация: Состояние почтового ящика синхронизируется между сервером и клиентским устройством.
- Оффлайн режим: Работа с письмами возможна в оффлайн-режиме.
- Управление письмами: Можно создавать папки и управлять письмами на сервере.

POP3 (Post Office Protocol version 3):
- Хранение: Сообщения загружаются на клиентское устройство и могут быть удалены с сервера.
- Синхронизация: Нет синхронизации состояния между сервером и клиентским устройством.
- Оффлайн режим: Требует подключения к серверу для просмотра писем.

2 Практические задание

2.1 Задание 1

TODO

Попробуйте отправить письмо на вашу почту (mail, yandex, gmail, etc) используя команду openssl (узнаете в DNS имя почтового сервера, подключаетесь к нему по нужному порту итд)

Подготавливаем данные для авторизации:

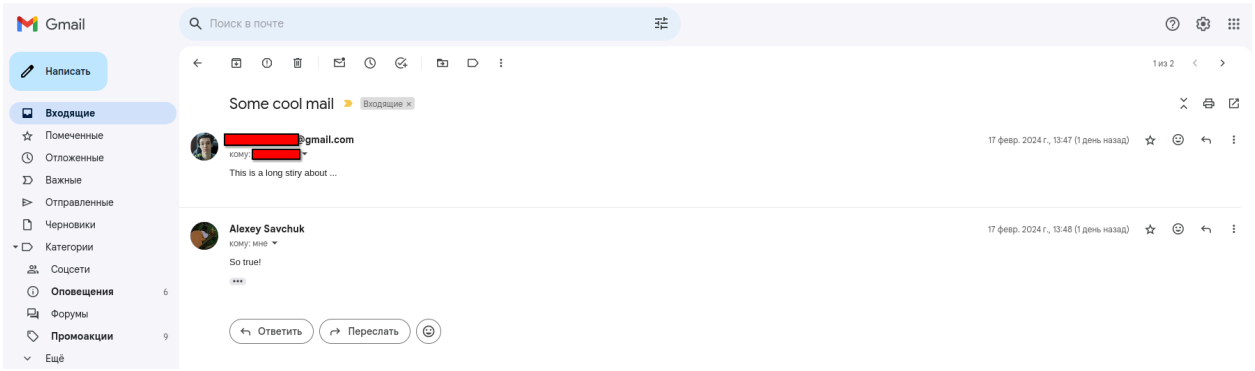
```
echo -n 'your_email@gmail.com' | openssl enc -base64
echo -n 'your_password' | openssl enc -base64
```

Авторизуемся и отправляем письмо:

```
250 SMTPUTF8
AUTH LOGIN
334 VXNlcm5hbWU6
<mail_base_64>
334 UGFzc3dvcmQ6
<pass_base_64>
235 2.7.0 Accepted
MAIL FROM: <some@gmail.com>
250 2.1.0 OK l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp
rcpt to: <another@gmail.com>
250 2.1.5 OK l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp
data
354  Go ahead l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp
from: some@gmail.com
to: another@gmail.com
subject: Some cool mail

This is a long stiry about ...
.
250 2.0.0 OK  1708166862 l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp
```

Смотрим через gmail



Разберем каждую часть.

1. **250 SMTPUTF8**: Это код ответа от сервера, который указывает, что сервер поддерживает расширение SMTPUTF8 для кодировки Unicode.

2. **AUTH LOGIN**: Это команда, которая инициирует процесс аутентификации. Когда вы видите эту команду, сервер ожидает от вас базовые данные для аутентификации.
3. **334 VXNlcm5hbWU6** и **334 UGFzc3dvcmQ6**: Это вызов для ввода имени пользователя (пользовательский адрес электронной почты) и пароля. Данные кодированы в формате Base64. Таким образом, вы должны ввести имя пользователя и пароль в закодированном виде.
4. **235 2.7.0 Accepted**: Это код ответа, который сообщает, что аутентификация прошла успешно, и сервер принимает команды.
5. **MAIL FROM:<some@gmail.com>**: Эта команда указывает адрес отправителя.
6. **250 2.1.0 OK l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp**: Это подтверждение от сервера о том, что адрес отправителя принят.
7. **RCPT TO: <another@gmail.com>**: Эта команда указывает адрес получателя.
8. **250 2.1.5 OK l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp**: Это подтверждение от сервера о том, что адрес получателя принят.
9. **DATA**: Эта команда сообщает серверу о начале передачи данных письма.
10. **354 Go ahead l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp**: Сервер готов принимать тело письма. Все данные, введенные после этой команды, будут считаться телом письма.
11. Затем идет само письмо с полями, такими как **«from»**, **«to»**, **«subject»** и текстом письма.
12. **.**: Это команда завершает передачу данных письма.
13. **250 2.0.0 OK 1708166862 l25-20020ac24a99000000b005115fc3d7f8sm228983lfp.205 - gsmtp**: Сервер подтверждает успешное получение и обработку письма.

2.2 Задание 2

TODO

Подключитесь по IMAP/POP3 к своему почтовому ящику, узнайте информацию о нем, используя команды протоколов

2.2.1 IMAP

```
openssl s_client -connect imap.gmail.com:993 -crlf -quiet
Connecting to 173.194.221.108
depth=2 C=US, O=Google Trust Services LLC, CN=GTS Root R1
verify return:1
depth=1 C=US, O=Google Trust Services LLC, CN=GTS CA 1C3
verify return:1
depth=0 CN=imap.gmail.com
verify return:1
* OK Gimap ready for requests from 178.71.185.95 c9mb22601693ltc
a login some@gmail.com "pass"
* CAPABILITY IMAP4rev1 UNSELECT IDLE NAMESPACE QUOTA ID XLIST CHILDREN X-GM-EXT-1
UIDPLUS COMPRESS=DEFLATE ENABLE MOVE CONDSTORE ESEARCH UTF8=ACCEPT LIST-EXTENDED LIST-
STATUS LITERAL- SPECIAL-USE APPENDLIMIT=35651584
a OK some@gmail.com authenticated (Success)
a status INBOX (MESSAGES RECENT UNSEEN)
* STATUS "INBOX" (MESSAGES 17 RECENT 0 UNSEEN 15)
a OK Success
```

Разберем каждую часть.

1. **openssl s_client -connect imap.gmail.com:993 -crlf -quiet**: Эта команда использует OpenSSL для установки защищенного SSL/TLS соединения с почтовым сервером Gmail на порту 993, который является стандартным портом для протокола IMAP.
2. После установки соединения, сервер возвращает сертификаты SSL, которые клиент (в данном случае OpenSSL) проверяет на валидность.
3. **OK Gimap ready for requests from 178.71.185.95 c9mb22601693ltc**: Сервер приветствует клиента и готов принимать запросы. IP-адрес и некоторая информация о клиенте также предоставляются.
4. **a login some@gmail.com «pass»**: Клиент отправляет команду на аутентификацию. В данном случае, имя пользователя (some@gmail.com) и пароль («pass») передаются в виде аргументов команды.
5. **CAPABILITY IMAP4rev1 UNSELECT IDLE NAMESPACE QUOTA ID XLIST CHILDREN X-GM-EXT-1 UIDPLUS COMPRESS=DEFLATE ENABLE MOVE CONDSTORE ESEARCH UTF8=ACCEPT LIST-EXTENDED LIST-STATUS LITERAL- SPECIAL-USE APPENDLIMIT=35651584**: Сервер отвечает, предоставляя список поддерживаемых возможностей (CAPABILITY) в рамках протокола IMAP. Это включает различные расширения, такие как IDLE, UIDPLUS, COMPRESS=DEFLATE и другие.
6. **a OK some@gmail.com authenticated (Success)**: Сервер подтверждает успешную аутентификацию пользователя.
7. **a status INBOX (MESSAGES RECENT UNSEEN)**: Клиент отправляет команду для запроса статуса почтового ящика INBOX. Сервер возвращает информацию о количестве сообщений, недавно полученных и непрочитанных в ящике.
8. **STATUS «INBOX» (MESSAGES 17 RECENT 0 UNSEEN 15)**: Сервер предоставляет статус ящика INBOX с указанием количества сообщений, недавно полученных, и непрочитанных.
9. **a OK Success**: Сервер подтверждает успешное выполнение команды status и возвращает статус «Success».

2.2.2 POP 3

```
openssl s_client -connect pop.gmail.com:995 -crlf -quiet

Connecting to 64.233.163.108
depth=2 C=US, O=Google Trust Services LLC, CN=GTS Root R1
verify return:1
depth=1 C=US, O=Google Trust Services LLC, CN=GTS CA 1C3
verify return:1
depth=0 CN=pop.gmail.com
verify return:1
+OK Gpop ready for requests from 178.71.185.95 w20mb22708066ltc
USER some@gmail.com
+OK send PASS
PASS <pass>
+OK Welcome.
LIST
+OK 276 messages (626188523 bytes)
1 3294
2 3749
3 3907
...
271 15832
```

```
272 14670
273 5151
274 5151
275 5975
276 5975
.
STAT
+OK 276 626188523
RETR 1
+OK message follows
MIME-Version: 1.0
Received: by 10.49.58.100; Fri, 24 Aug 2012 01:22:20 -0700 (PDT)
Date: Fri, 24 Aug 2012 01:22:20 -0700
Message-ID: <CAByGqTDkcAV+QQDdnqUC+U8tZ=n8256=T793BvS0qffc7yoZ9A@mail.gmail.com>
Subject: =?KOI8-R?B?6dPQz8zY2tXK1MUgR21haWwgzsEg08/Uz9fPzSDU?=
        =?KOI8-R?B?xczFxs/OxQ==?=
From: =?KOI8-R?B?68/MzMXL1MnXIEdtYWls?= <mail-noreply@google.com>
To: =?KOI8-R?B?98HEyc0g8dLP18/K?= <some@gmail.com>
Content-Type: multipart/alternative; boundary=e89a8f921a22babddc04c7feac1d
```

Разберем каждую часть.

1. **openssl s_client -connect pop.gmail.com:995 -crlf -quiet**: Эта команда использует OpenSSL для установки защищенного SSL/TLS соединения с почтовым сервером Gmail на порту 995, который является стандартным портом для протокола POP3 с использованием шифрования.
2. После установки соединения, сервер возвращает сертификаты SSL, которые клиент (в данном случае OpenSSL) проверяет на валидность.
3. **+OK Gpop ready for requests from 178.71.185.95 w20mb22708066ltc**: Сервер приветствует клиента и готов принимать запросы. IP-адрес и некоторая информация о клиенте также предоставляются.
4. **USER some@gmail.com**: Клиент отправляет команду на аутентификацию пользователя, указывая имя пользователя (some@gmail.com).
5. **+OK send PASS**: Сервер подтверждает получение имени пользователя и ожидает команды для отправки пароля.
6. **PASS** : Клиент отправляет свой пароль в зашифрованном виде.
7. **+OK Welcome.**: Сервер подтверждает успешную аутентификацию пользователя.
8. **LIST**: Клиент запрашивает список сообщений на сервере.
9. **+OK 276 messages (626188523 bytes)**: Сервер отвечает, сообщая об общем количестве сообщений и их общем размере.
10. **1 3294, 2 3749, …, 276 5975**: Сервер предоставляет список сообщений с номерами и их размерами.
11. **STAT**: Клиент запрашивает статистику по почтовому ящику.
12. **+OK 276 626188523**: Сервер отвечает, предоставляя информацию о количестве сообщений и их общем размере.
13. **RETR 1**: Клиент запрашивает текст первого сообщения.
14. **+OK message follows**: Сервер подтверждает и готов отправить содержимое сообщения.
15. Затем идет фрагмент текста письма

3 Вывод

В процессе выполнения команд были установлены защищенные SSL/TLS соединения с серверами Gmail для протоколов IMAP, SMTP и POP3. Затем произведена аутентификация почтового ящика, выполнены запросы о статусе почтового ящика, получен список сообщений, а также извлечено и отображено содержимое одного из писем в формате MIME.