

Санкт-Петербургский политехнический университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Разработка сетевых приложений

Отчет по лабораторной работе

"Изучение прикладных протоколов в командной строке Linux"

Работу

выполнил:

Кнорре А.В.

Группа: 43501/3

Преподаватель:

Зозуля А.В.

Санкт-Петербург
2019

Содержание

1. Цель работы	3
2. Программа работы	3
3. Ход выполнения работы	3
3.1. SMTP	3
3.1.1. Основные сведения	3
3.1.2. Основные команды	3
3.1.3. Область применения	4
3.1.4. Консоль	4
3.2. POP3	4
3.2.1. Основные сведения	4
3.2.2. Основные команды	5
3.2.3. Область применения	5
3.2.4. Консоль	5
3.3. IMAP	6
3.3.1. Основные сведения	6
3.3.2. Основные команды	7
3.3.3. Область применения	7
3.3.4. Консоль	7
3.4. HTTP	8
3.4.1. Основные сведения	8
3.4.2. Методы	8
3.4.3. Коды ответов	9
3.4.4. Область применения	9
3.4.5. Консоль	9
3.5. FTP	9
3.5.1. Основные сведения	9
3.5.2. Активный режим	9
3.5.3. Пассивный режим	10
3.5.4. Основные команды	10
3.5.5. Область применения	10
3.5.6. Консоль	11
3.6. TFTP	12
3.6.1. Основные сведения	12
3.6.2. Типы пакета	12
3.6.3. Режимы передачи	12
3.6.4. Область применения	12
3.6.5. Консоль	12
3.7. WebDAV	13
3.7.1. Основные сведения	13
3.7.2. Новые методы	13
3.7.3. Область применения	13
3.7.4. Консоль	14
4. Выводы	14

1. Цель работы

Познакомиться с основами прикладными протоколами используя средства командной строки Linux.

2. Программа работы

- SMTP. При помощи утилиты telnet* отправить email через SMTP-сервер Yandex.
- POP3. При помощи утилиты telnet* прочитать email при помощи POP3-сервера Yandex.
- IMAP. При помощи утилиты telnet* прочитать email при помощи IMAP-сервера Yandex.
- HTTP. При помощи утилиты telnet* прочитать главную страницу сайта yandex.ru.
- FTP. При помощи утилиты telnet загрузить файл с FTP-сервера ftp.sunet.se
- TFTP. При помощи утилиты netcat выяснить имя файла, который запрашивает удаленный хост (при помощи утилиты tftp) у данного хоста.
- WebDAV. При помощи утилиты curl загрузить файл, создать директорию, выгрузить файл на сервис disk.yandex.ru.

3. Ход выполнения работы

3.1. SMTP

3.1.1. Основные сведения

- Simple Mail Transfer Protocol.
- Протокол передачи электронной почты.
- Использует TCP, порт 25.
- Не поддерживает шифрования.
- Базовая версия не поддерживает аутентификацию.
- Спецификация RFC 2554 реализуется как расширение SMTP. Ответ на EHLO - список поддерживаемых механизмов аутентификации

3.1.2. Основные команды

- HELO <домен>
- MAIL FROM: <адрес>
- RCPT TO: <адрес>
- DATA
- QUIT

3.1.3. Область применения

Обмен почтовыми сообщениями без шифрования, то есть личная переписка без персональных и коммерческих данных.

3.1.4. Консоль

```
alexander@alexander-ThinkPad-T420s:~$ openssl s_client -connect smtp.yandex.ru:25 -start
<...>
AUTH LOGIN
334 VXNlcm5hbWU6
bnV0dHlydW5uZXI=
334 UGFzc3dvcmQ6
<BASE64 моего пароля>
235 2.7.0 Authentication successful.
mail from: nuttyrunner@yandex.ru
250 2.1.0 <nuttyrunner@yandex.ru> ok
rcpt to: nuttyrunner@gmail.com
250 2.1.5 <nuttyrunner@gmail.com> recipient ok
DATA
354 Enter mail, end with "." on a line by itself
From: nuttyrunner@yandex.ru
To: nuttyrunner@gmail.com
Subject: Welcome

Hello, my friend
.
250 2.0.0 Ok: queued on smtp4o.mail.yandex.net as 1550418119-FLDqfG15Px-fC04oq3n
```

3.2. POP3

3.2.1. Основные сведения

- Post Office Protocol, версия 3.
- Протокол доступа к удалённому почтовому ящику.
- Использует TCP, порт 110.
- Не поддерживает шифрования.
- Аутентификация пользователя.
- Просмотр списка писем.
- Копирование писем в локальный ящик.
- Удаление писем с сервера.
- Ящик представляется одной почтовой папкой (Inbox).

3.2.2. Основные команды

- USER <имя> -> -ERR или +OK
- PASS <пароль> -> -ERR или +OK
- STAT -> +OK <число писем> <общая длина>
- LIST -> +OK 1..N <длины писем>
- RETR <number> -> +OK <текст сообщения> . или -ERR
- DELE <N> -> +OK или -ERR
- QUIT -> +OK

3.2.3. Область применения

Незащищённое чтение сообщений из почтового ящика без возможности категоризации писем с помощью каталогов или фильтров.

3.2.4. Консоль

```
alexander@alexander-ThinkPad-T420s:~$ openssl s_client -crlf -ign_eof -connect pop.yandex.ru
CONNECTED(00000003)
<...>
+OK POP Ya! na@28p 3NUq20w3dCg1
user nuttyrunner
+OK password, please.
pass <мой пароль>
+OK 105 1155023
list
+OK 105 1155023
1 2976
2 2399
<...>
104 8049
105 1703
.
retr 105
+OK 1703 octets.
X-Yandex-FolderName: Inbox
Received: from mxback6j.mail.yandex.net ([127.0.0.1])
by mxback6j.mail.yandex.net with LMTP id 8MsNb46j
for <nuttyrunner@yandex.com>; Sun, 17 Feb 2019 19:22:55 +0300
Received: from mxback6j.mail.yandex.net (localhost.localdomain [127.0.0.1])
by mxback6j.mail.yandex.net (Yandex) with ESMTTP id 291AE53C14C3
for <nuttyrunner@yandex.com>; Sun, 17 Feb 2019 19:22:55 +0300 (MSK)
X-Yandex-Internal: 1
Received: from smtp4p.mail.yandex.net (smtp4p.mail.yandex.net [2a02:6b8:0:1402::15:6])
by mxback6j.mail.yandex.net (nwsmtpp/Yandex) with ESMTTP id zkpxsKgpVv-MtbqM9gt;
Sun, 17 Feb 2019 19:22:55 +0300
X-Yandex-Front: mxback6j.mail.yandex.net
```

X-Yandex-TimeMark: 1550420575
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=yandex.ru; s=mail; t=1550420575;
bh=dvq1MPvNC+UUn6WXz0eHefYShSdkA00farn93A4MAZU=;
h=Message-Id:Date:From:To:Subject;
b=PbHJAoqVZPSJuSpacrD0bhl548Se5MQ1nmuq/bJzhW+J6n8NGrT7TirT7UJf/84Lh
1Hbsz0DarJ9zXoLT0oEcogYcntVd4hqpbklLZKmtGJAQg+05SBakKZS+zVtQ71zrEP
OtkAJpmTyIOF/mwQZJQ49ysL4/x9lVNVabxl5eoY=
Authentication-Results: mxback6j.mail.yandex.net; dkim=pass header.i=@yandex.ru
Received: by smtp4p.mail.yandex.net (nwsmtп/Yandex) with ESMTPSA id eErCVwTwoQ-MIBmqKcg;
Sun, 17 Feb 2019 19:22:27 +0300
(using TLSv1.2 with cipher ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits))
(Client certificate not present)
X-Yandex-Front: smtp4p.mail.yandex.net
X-Yandex-TimeMark: 1550420547
Message-Id: <20190217192254.MIBmqKcg@smtp4p.mail.yandex.net>
Date: Sun, 17 Feb 2019 19:22:54 +0300
X-Yandex-Spam: 1
From: nuttyrunner@yandex.ru
To: nuttyrunner@yandex.com
Subject: Welcome
Return-Path: nuttyrunner@yandex.ru

Hello there!

.

3.3. IMAP

3.3.1. Основные сведения

- Internet Mail Access Protocol, версия 4.
- Создан как альтернатива POP-3.
- Использует TCP, порт 143.
- Варианты аутентификации (login и authenticate).
- Позволяет хранить удаленную структуру папок сообщений.
- Обеспечивает асинхронный обмен командами.
- Уникальный номер команды и ответа.
- Флаги сообщений.
- Уникальные идентификаторы сообщений.
- Механизмы копирования и перемещения сообщений.
- Средства поиска сообщений.

3.3.2. Основные команды

- CAPABILITY - запрос списка возможностей
- LOGOUT
- LOGIN <username> <password>
- AUTHENTICATE <method>
- SELECT <имя ящика> - выбор ящика
- EXAMINE <имя ящика> - выбор ящика (RO)
- CREATE <имя ящика> - создание ящика
- DELETE <имя ящика> - удаление ящика
- RENAME <имя ящика> <новое имя> - переименование ящика
- SUBSCRIBE <имя ящика> - подписка на ящик
- UNSUBSCRIBE <имя ящика> - отмена подписки на ящик
- LIST <база> <имя ящика> - выдача списка ящиков
- LSUB <база> <имя ящика> - выдача списка подписанных ящиков
- STATUS <имя ящика> [<имена элементов состояния>] - выдача состояния ящика
- APPEND <имя ящика> [<флаги>] - добавить сообщение в ящик
- CHECK - проверка ящика
- CLOSE - удаление помеченных сообщений и закрытие ящика
- SEARCH [CHARSET] <критерии> - поиск сообщения
- FETCH <набор сообщений> <элементы данных>
- COPY <набор сообщений> <имя ящика> - копирование сообщений в ящик

3.3.3. Область применения

Чтение сообщений из почтового ящика с возможностью категоризации писем с помощью каталогов и фильтров.

3.3.4. Консоль

```
alexander@alexander-ThinkPad-T420s:~$ openssl s_client -connect imap.yandex.ru:993 -crlf
CONNECTED(00000003)
<...>
* OK Yandex IMAP4rev1 at imap53p.mail.yandex.net:993 ready to talk with ::ffff:109.167.1
a1 LOGIN nuttyrunner@yandex.ru ПАОПЛЬ
* CAPABILITY IMAP4rev1 CHILDREN UNSELECT LITERAL+ NAMESPACE XLIST BINARY UIDPLUS ENABLE
a1 OK LOGIN Completed.
a2 select inbox
* FLAGS (\Answered \Seen \Draft \Deleted $Forwarded)
```

```

* 105 EXISTS
* 26 RECENT
* OK [UNSEEN 7]
* OK [PERMANENTFLAGS (\Answered \Seen \Draft \Flagged \Deleted $Forwarded \*)] Limited
* OK [UIDNEXT 107] Ok
* OK [UIDVALIDITY 1436313945] Ok
a2 OK [READ-WRITE] select Completed.
a2 FETCH 105 full
* 105 FETCH (FLAGS (\Seen encrypted) BODY ("TEXT" "PLAIN" NIL NIL NIL "7BIT" 14 1) ENVELOPE)
a2 OK FETCH Completed.
a2 FETCH 105 BODY[TEXT]
* 105 FETCH (BODY[TEXT] {14}
Hello there!
)
a2 OK FETCH Completed.

```

3.4. HTTP

3.4.1. Основные сведения

- Hyper Text Transfer Protocol.
- Протокол передачи файлов, объектов.
- Использует TCP, порт 80.

Формат HTTP-запроса:

- <Request-line> - строка запроса
- <General-header> - общий заголовок
- <Request-header> - заголовок запроса
- <Entity-header> - заголовок сообщения
- <Body> - тело

Формат: <METHOD> <URL> <HTTP-VERSION>

3.4.2. Методы

- GET
- POST
- HEAD
- PUT
- DELETE
- OPTIONS
- UPDATE

3.4.3. Коды ответов

- 1xx - информационные
- 2xx - ОК
- 3xx - переадресация
- 4xx - ошибка клиента
- 5xx - ошибка сервера

3.4.4. Область применения

Удалённое сообщение в сфере веб-технологий в виде самых различных запросов информации к серверам, реализующим сервисы по указанию широкого спектра услуг, к примеру - поисковик.

3.4.5. Консоль

```
alexander@alexander-ThinkPad-T420s:~$ telnet yandex.ru 80
Trying 77.88.55.70...
Connected to yandex.ru.
Escape character is '^]'.
GET / HTTP/1.1
Host: yandex.ru
```

```
HTTP/1.1 302 Found
```

```
Date: Sun, 17 Feb 2019 18:01:01 GMT
```

```
Cache-Control: no-cache,no-store,max-age=0,must-revalidate
```

```
Location: https://yandex.ru/
```

```
Expires: Sun, 17 Feb 2019 18:01:02 GMT
```

```
Last-Modified: Sun, 17 Feb 2019 18:01:02 GMT
```

```
P3P: policyref="/w3c/p3p.xml", CP="NON DSP ADM DEV PSD IVDo OUR IND STP PHY PRE NAV UNI"
```

```
Set-Cookie: yandexuid=8974430671550426461; Expires=Wed, 14-Feb-2029 18:01:01 GMT; Domain=
```

```
X-Content-Type-Options: nosniff
```

```
Content-Length: 0
```

3.5. FTP

3.5.1. Основные сведения

- File Transfer Protocol.
- Использует транспорт TCP.
- Поддерживает два режима передачи.

3.5.2. Активный режим

- Режим «по умолчанию».
- Сервер инициирует соединение данных.
- Клиент открывает слушающий порт.

- Номер TCP-порта сервера – 20.
- Невозможно использовать с технологиями типа NAT, Proxy.
- Обычно запрещён в межсетевых экранах.

3.5.3. Пассивный режим

- Клиент инициирует соединение данных.
- Сервер информирует о параметрах канала данных.
- Сервер открывает слушающий порт.
- Поддерживается не всеми реализациями.

3.5.4. Основные команды

- USER <имя>
- PASS <пароль>
- ABOR
- QUIT
- DELE <имя> - удалить файл
- RNFR <имя> - переименовать из
- RNT0 <имя> - переименовать в
- RMD <имя> - удалить каталог
- MKD <имя> - создать каталог
- PWD - текущий каталог
- PORT a1, a2, a3, a4, p1, p2 (перевод в активный режим, порт $p1 * 256 + p2$)
- PASV - перевод в пассивный режим
- TYPE A | E | I - ASCII / EDCDIC / Image
- MODE S | B | C - режим передачи данных Stream / Block / Compressed
- RETR <имя> - получить файл
- STOR <имя> - записать файл
- LIST [<путь>] - получить список файлов с атрибутами
- NLST [<путь>] - получить список имён файлов

3.5.5. Область применения

Простота при размещении в рамках хранилища института или прочего применения с назначением эффективного предоставления доступа к информации с минимальными требованиями к конфиденциальности.

3.5.6. Консоль

```
alexander@alexander-ThinkPad-T420s:~$ ftp ftp.sunet.se
Connected to sunet.ftp.acc.umu.se.
220 Please use http://ftp.acc.umu.se/ whenever possible.
Name (ftp.sunet.se:alexander): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pass
Passive mode on.
ftp> ls
227 Entering Passive Mode (194,71,11,173,154,85).
150 Here comes the directory listing.
-rw-r--r--      1 ftp      ftp      1216 Jun 02  2017 HEADER.html
lrwxrwxrwx      1 ftp      ftp           3 Mar 16  2010 Public -> pub
drwxr-xr-x      3 ftp      ftp      10 Jun 30  2017 about
drwxr-sr-x     30 ftp      ftp      33 Feb 16 22:31 cdimage
drwxr-xr-x      2 ftp      ftp           3 Jun 14  2006 conspiracy
lrwxrwxrwx      1 ftp      ftp      22 Mar 16  2010 debian -> cdimage/.debian-mirror
drwxr-xr-x      5 ftp      ftp           7 Mar 13  2016 debian-backports
lrwxrwxrwx      1 ftp      ftp      16 Mar 16  2010 debian-cd -> cdimage/release/
-rw-r--r--      1 ftp      ftp    15086 Apr 02  2018 favicon.ico
drwxr-xr-x     82 ftp      ftp      89 Feb 04 20:28 mirror
drwxr-xr-x      4 ftp      ftp      12 Feb 05  2016 pub
lrwxrwxrwx      1 ftp      ftp      23 Mar 16  2010 releases -> mirror/ubuntu-releases
-rw-r--r--      1 ftp      ftp    1859 Mar 23  2017 robots.txt
lrwxrwxrwx      1 ftp      ftp      12 Aug 01  2016 tails -> mirror/tails
lrwxrwxrwx      1 ftp      ftp      13 Mar 16  2010 ubuntu -> mirror/ubuntu
226 Directory send OK.
ftp> cd about
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (194,71,11,173,136,75).
150 Here comes the directory listing.
-rw-r--r--      1 ftp      ftp     2798 May 07  2007 ftp-about-SPmkII.html
-rw-r--r--      1 ftp      ftp     3200 Oct 04  2016 ftp.sunet.se-history_sv.html
-rw-r--r--      1 ftp      ftp     2550 May 07  2007 graph.png
-rw-r--r--      1 ftp      ftp     6863 Jun 30  2017 index.html
-rw-r--r--      1 ftp      ftp     2550 May 07  2007 largefile.png
-rw-r--r--      1 ftp      ftp     1558 May 07  2007 smallcachedfile.png
-rw-r--r--      1 ftp      ftp     2545 May 07  2007 smalluncachedfile.png
drwxr-xr-x      2 ftp      ftp           31 Nov 14  2012 zfs-stats
226 Directory send OK.
ftp> get graph.png
local: graph.png remote: graph.png
227 Entering Passive Mode (194,71,11,173,125,212).
150 Opening BINARY mode data connection for graph.png (2550 bytes).
226 Transfer complete.
```

2550 bytes received in 0.00 secs (10.5733 MB/s)

3.6. TFTP

3.6.1. Основные сведения

- Trivial File Transfer Protocol.
- Не поддерживает аутентификацию.
- Основан на протоколе UDP, порт 69.

3.6.2. Типы пакета

- Read Request (RRQ, 1) – запрос на чтение файла.
- Write Request (WRQ, 2) – запрос на запись файла.
- Data (DATA, 3) – данные, передаваемые через TFTP.
- Acknowledgment (ACK, 4) – подтверждение пакета.
- Error (ERR, 5) – ошибка.
- Option Acknowledgment (OACK, 6) – подтверждение опций.

3.6.3. Режимы передачи

- netascii – файл перед передачей перекодировается в ASCII.
- octet – файл передается без изменений.

3.6.4. Область применения

Предоставление удалённого доступа к файлам при полном отсутствии средств обеспечения конфиденциальности и безопасности с минимальными усилиями.

3.6.5. Консоль

Сервер:

```
alexander@alexander-ThinkPad-T420s:~$ sudo nc -ul 127.0.0.1 69
FILEnetasciifILEnetasciifILEnetasciifILEnetasciifILEnetasciif
```

Где первый символ это 0x01, то есть поступают запросы на Read Request в режиме передачи

Клиент:

```
alexander@alexander-ThinkPad-T420s:~$ sudo tftp 127.0.0.1
tftp> get FILE
Transfer timed out.
```

3.7. WebDAV

3.7.1. Основные сведения

- Web Distributed Authoring and Versioning.
- Набор расширений и дополнений к протоколу HTTP, поддерживающих совместную работу пользователей над редактированием файлов и управление файлами на удаленных веб-серверах.
- Блокировка – долгосрочные блокировки на запись документа предотвращают потерю информации при одновременном редактировании документа несколькими пользователями.
- Свойства – произвольные метаданные могут храниться в качестве свойств, описанных на языке XML. В качестве примера можно привести список авторов документа или его краткую аннотацию. Протокол DAV предоставляет средства для создания, редактирования и удаления свойств. Протокол DASL или DAV Searching and Locating предоставляет средства поиска и локализации веб-ресурсов на основе значения их свойств.
- Именованные области (Namespace) – Раздел DAV, поддерживающий переименование и перемещение веб-ресурсов. Механизм реализован в протоколе с помощью коллекций, выполняющих функцию, аналогичную папкам в файловой системе.

3.7.2. Новые методы

- PROPFIND – Получение свойств объекта на сервере в формате XML. Также можно получать структуру репозитория (дерево каталогов).
- PROPPATCH – Изменение свойств за одну транзакцию.
- MKCOL – Создать коллекцию объектов (каталог в случае доступа к файлам).
- COPY – Копирование из одного URI в другой.
- MOVE – Перемещение из одного URI в другой.
- LOCK – Поставить блокировку на объекте. WebDAV поддерживает эксклюзивные и общие (shared) блокировки.
- UNLOCK – Снять блокировку с ресурса.

3.7.3. Область применения

DAV применяется в качестве сетевой файловой системы, эффективной для работы в Интернете и способной обрабатывать файлы целиком, поддерживая хорошую производительность работы в условиях окружения с высокой временной задержкой передачи информации. Кроме того, DAV широко применяется в качестве протокола для доступа через Интернет и манипулирования содержимым систем документооборота (document management system).

3.7.4. Консоль

Создадим папку

```
alexander@alexander-ThinkPad-T420s:~$ curl -X MKCOL --user "nuttyrunner:ПАРОЛЬ" https://
```

Создадим локальный файл

```
alexander@alexander-ThinkPad-T420s:~$ echo bla bla bla > text.txt
```

Создадим удалённый файл с таким же содержанием

```
alexander@alexander-ThinkPad-T420s:~$ curl -T ./text.txt --user "nuttyrunner:ПАРОЛЬ" htt
```

Скачаем наш файл

```
alexander@alexander-ThinkPad-T420s:~$ curl -O --user "nuttyrunner:ПАРОЛЬ" https://webdav
```

% Total		% Received		% Xferd		Average Speed		Time	Time	Time	Current
						Dload	Upload	Total	Spent	Left	Speed
100	12	100	12	0	0	61	0	--:--:--	--:--:--	--:--:--	61

```
alexander@alexander-ThinkPad-T420s:~$
```

4. Выводы

Выполнение данной работы дало возможность закрепить теоретические знания о прикладных протоколах на практике. Для этого мы воспользовались консолью Linux чтобы произвести базовые операции над основными прикладными протоколами, предложенными преподавателем.

Полученные знания помогут при самостоятельной реализации данных протоколов, в частности при тестировании разработанных серверных и клиентских приложений.