Базовое Администрирование Linux

Занятие 10

Дмитрий Молчанов

Почта, что нужно знать

1. Протоколы почты SMTP, POP3/IMAP
2. Методы борьбы со спамом.
3. Установка/настройка:
    1. smtp-сервера
    2. imap/pop3-сервера

Компоненты почтовых систем

- MTA – Mail Transfer Agent, агент передачи сообщений – чаще всего smtp-сервер.
- MDA – Mail Delivery Agent, агент доставки сообщений – чаще всего POP3/IMAP сервер
- MUA – Mail User Agent – почтовый клиент

Роли почтовых серверов

- Emitter – только отправляет почту, не принимает
- SmartHost/Relay - сервер который занимается передачей почты во вне, т.е. принимает, передает, но сам не хранит
- MailService – клиентский сервис, принимает почту от других хостов и клиентов, отправляет, доставляет клиентам.

SMTP

Протокол SMTP (Simple Mail Transfer Protocol) является простым, текстовым, диалоговым протоколом.

Как понятно из названия – протокол служит для передачи потовых сообщений. Для своей работы он использует следующие порты:

- 25/tcp – smtp
- 465/tcp – smtps (smtp over ssl)

Основные атрибуты протокола

- Адрес клиента
- имя клиента
- атрибуты «конверта»
  - отправитель
  - Получатель

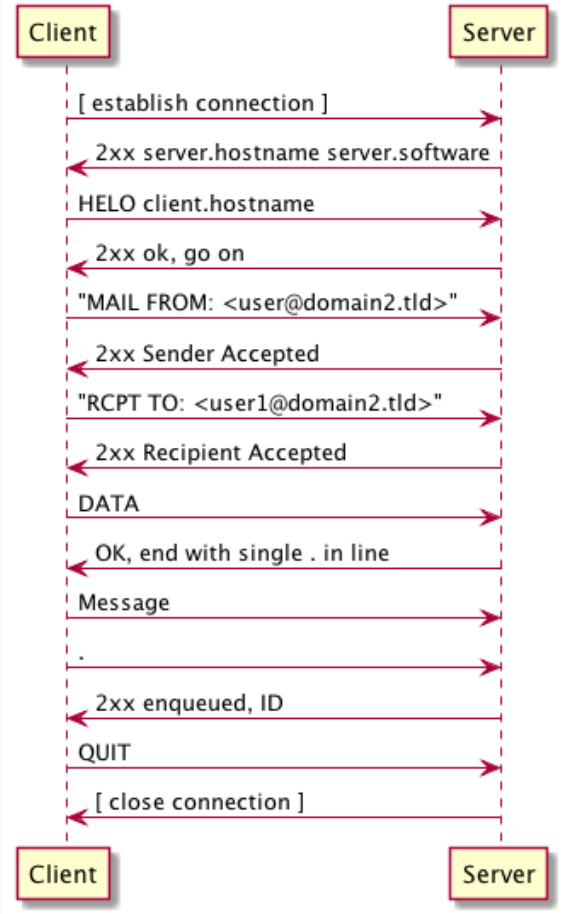
Основные команды протокола

- HELO/EHLO (Extended HELO) – приветствие
- MAIL FROM - указание отправителя
- RCPT TO – указание получателя
- DATA – Указание того, что дальше пойдет тело письма, содержимое конверта
- AUTH – аутентификация

Коды ответов сервера:

- 2xx – Положительный ответ
- 4xx – временная (мягкая) ошибка
- 5xx – постоянная (жесткая) ошибка

Диаграмма работы протокола smtp



POP3/IMAP

POP3 – Post Office Protocol v.3

IMAP – Internet Message Access Protocol

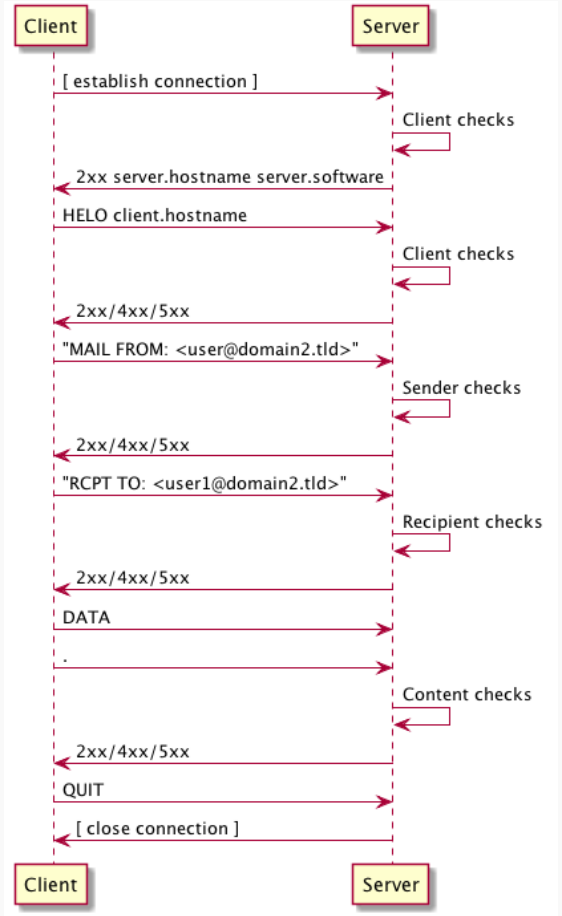
Оба протокола являются протоколами получения почты.

Методы борьбы со спамом.

Рубежи обороны:

- Предварительная фильтрация
- Проверки клиента
- Проверки отправителя
- Проверки получателя
- Проверки содержимого

Рубежи обороны



Общие проверки

- **RFC Compliance** соотвествие RFC в протоколе.
  Протоколы, точнее их реализации позволяют «вольности». Многие спамеры этим пользуются, по этому их можно отфильтровать.

Client Checks

- Local blacklists
- DNSBL
- helo-hostname -> ip -> reverse mapping
- reverse mapping checks
  - *-*-*-*.broadband.some.provider.ru
- Relay access
- SPF

Sender Checks

- Sender validation
  - reverse connect
  - DNS lookup
- RHSBL (Right Hand Side BL) DNSBL

Recipient Checks

- Recipient Existence
- RHSBL

Greylisting

- Триплет: Client+Sender+Recipient

при каждой попытке отправить сообщение сервер проверяет у грейлистера – Использовался ли такой триплет. Если использовался – принимаем сообщение, если нет - посылаем 4xx, мягкую, ошибку.

Суть в том, что спамеры постоянно пытаются слать с разных хостов ботнета, а легитимный клиент перепошлет сообщение через какой-то интервал (10 минут например). В итоге спамер не сможет послать письмо, т.к. будет постоянно использовать новый триплет за счет

Анализ контента

Наиболее тяжелые методы проверки, т.к. требуют анализа письма целиком, что может быть накладным из-за размеров письма.

Делятся на 2 типа:

- Проверка заголовков письма
  - DKIM
  - Фильтры по заголовкам
- Проверка тела письма:
  - Антивирусы
  - Различные антиспамовые алгоритмы DCC, Bayes.

Программное обеспечение почтовых систем

- MTA
  - postfix
  - sendmail
  - qmail
- MDA
  - courier-imap
  - dovecot
- MUA
  - WebMail
  - Outlook, Thunderbird

Ключевые параметры:

- myhostname
- mydestination
- myorigin
- mynetworks
- inet_intrefaces

Установка и настройка postfix

конфигурация:

- /etc/postfix
  - main.cf – основные параметры
  - master.cf – управление процессами