Простейший SOCKS сервер

М.И. Костенчук

06-06-2010

Содержание

1 Введение

Целью работы является написание простейшего SOCKS-сервера, обрабатывающего TCP/IP соединение.

2 Протокол SOCKS 5

Соединение с SOCKS-сервером происходит следующим образом:

1. Клиент подключается, и посылает приветствие, которое включает перечень поддерживаемых методов аутентификации
2. Сервер выбирает из них один (или посылает ответ о неудаче запроса, если ни один из предложенных методов не приемлем)
3. В зависимости от выбранного метода, между клиентом и сервером может пройти некоторое количество сообщений
4. Клиент посылает запрос на соединение специального вида
5. Сервер отвечает аналогичным образом

Рассмотрим соединение подробней.
Первый запрос от клиента выглядит следующим образом:

VER	NMethods	Methods
1	1	1-255

Где первая строка это названия полей, а вторая их размер:

- VER — версия протокола. В нашем случае это поле равно 0x05.
- NMethods — Количество методов аутентификации.
- Methods — Методы аутентификации:

- 0x00 — аутентификация не требуется
- 0x01 — GSSAPI
- 0x02 — USERNAME/PASSWORD (см. RFC 1929)
- 0x03 до 0x7F — зарезервировано IANA
- 0x80 до 0xFE — предназначено для частных методов
- 0xFF — нет применимых методов

Сервер выбирает один из предложенных методов и посылает ответ в следующем виде:

VER	Method
1	1

Затем клиент и сервер начинают аутентификацию выбранным способом. Реализация аутентификации выходит за рамки данной работы, поэтому не будет рассмотрено.

После успешной аутентификации клиент посылает серверу запрос вида:

VER	CMD	RSV	AType	DST.Addr	DST.Port
1	1	1	1	переменное	2

- VER — Версия протокола
- CMD — Тип запроса:
  - 0x01 — Connect
  - 0x02 — Bind
  - 0x03 — UDP Associate
- AType — Тип адреса хоста:
  - 0x01 — IPv4
  - 0x03 — Имя домена
  - 0x04 — IPv6
- DST.Addr — Адрес хоста в виде, указанном в AType:
- DST.Port — Порт хоста

Сервер отправляет ответ вида:

VER	REP	RSV	AType	BND.Addr	BND.Port
1	1	1	1	переменное	2

- VER — Версия протокола
- REP — Код ответа:
  - 0x00 — Успешноый
  - 0x01 до 0x08 — Различные ошибки
- AType — Тип последующего адреса (аналогично запросу):
- DST.Addr — Выданный сервером адрес
- DST.Port — Выданный сервером порт

Если сервер ответил 0x00, значит значит соединение прошло успешно и можно отправлять данные.

3 Итог

Полностью реализовано соединение с клиентом. Обмен данными происходит следующим образом: Сервер ждёт сообщения от клиента, после его приёма полностью пересылает удалённому хосту, и пересылает ответ обратно клиенту. Для проверки реализован собственный простейший socks-клиент.

Список литературы

[1] `http://ru.wikipedia.org/wiki/SOCKS` — Википедия про SOCKS.

[2] `http://rfc2.ru/1928.rfc` — RFC 1928 — протокол SOCKS5.