Протокол FTP

FTP

- FTP (англ. File Transfer Protocol — протокол передачи файлов) — протокол, предназначенный для передачи файлов в компьютерных сетях. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами (см. FXP).

- FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. До начала 90-х годов на долю FTP приходилось около половины трафика в сети Интернет. Он и сегодня широко используется для распространения ПО и доступа к удалённым хостам.

- Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов передаются по разным портам. Порт 20 используется для передачи данных, порт 21 для передачи команд. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

Проблема безопасности FTP

- Протокол не шифруется, при аутентификации передаются логин и пароль открытым текстом. В случае построения сети с использованием хаба злоумышленник при помощи пассивного сниффера может перехватывать логины и пароли находящихся в том же сегменте сети пользователей FTP, или, при наличии специального ПО, получать передаваемые по FTP файлы без авторизации. Чтобы предотвратить перехват трафика, необходимо использовать протокол шифрования данных SSL, который поддерживается многими современными FTP-серверами и некоторыми FTP-клиентами.

Процесс авторизации FTP

- Процесс нешифрованной авторизации проходит в несколько этапов (символы \r\n означают перевод строки):

1. Установка TCP-соединения с сервером (обычно на 21 порт)
2. Посылка команды USER логин\r\n
3. Посылка команды PASS пароль\r\n

После успешной авторизации можно посылать на сервер другие команды.

Анонимный вход на FTP

- Если к серверу разрешён анонимный доступ (как правило, лишь для загрузки данных с сервера), то в качестве логина используется ключевое слово «anonymous» или «ftp», а в качестве пароля — адрес электронной почты:

1. USER anonymous\r\n
2. PASS someone@email\r\n

Основные команды протокола

- ABOR — Прервать передачу файла
- CDUP — Сменить директорию на вышестоящую.
- CWD — Сменить директорию.
- DELE — Удалить файл (DELE filename).
- EPSV - Войти в расширенный пассивный режим. Применяется вместо PASV.
- HELP — Выводит список команд принимаемых сервером.

Основные команды протокола

- LIST — Возвращает список файлов директории. Список передается через соединение данных (20 порт).
- MDTM — Возвращает время модификации файла.
- MKD — Создать директорию.
- NLST — Возвращает список файлов директории в более кратком формате чем LIST. Список передается через соединение данных (20 порт).
- NOOP — Пустая операция

Основные команды протокола

- PASV — Войти в пассивный режим. Сервер вернет адрес и порт к которому нужно подключиться чтобы забрать данные. Передача начнется при введении следующих команд RETR, LIST и тд.
- PORT — Войти в активный режим. Например PORT 12,34,45,56,78,89. В отличие от пассивного режима для передачи данных сервер сам подключается к клиенту.
- PWD — Возвращает текущую директорию.
- QUIT — Отключиться

Основные команды протокола

- REIN — Реинициализировать подключение
- RETR — Скачать файл. Перед RETR должна быть команда PASV или PORT.
- RMD — Удалить директорию
- RNFR и RNTO — Переименовать файл. RNFR — что переименовывать, RNTO — во что.
- SIZE — Возвращает размер файла

Основные команды протокола

- STOR — Закачать файл. Перед STOR должна быть команда PASV или PORT.
- SYST — Возвращает тип системы(UNIX, WIN, …)
- TYPE — Установить тип передачи файла(Бинарный, текстовый)
- USER — Имя пользователя для входа на сервер

Пример работы FTP

- 220 FTP server ready.
- USER ftp //Анонимус
- 230 Login successful.
- PASV
- 227 Entering Passive Mode (192,168,254,253,233,92)//Клиент должен открыть соединение на переданный IP
- LIST
- 150 Here comes the directory listing. //Сервер передает список файлов в директории
- 226 Directory send OK.
- CWD incoming
- 250 Directory successfully changed.
- PASV
- 227 Entering Passive Mode (192,168,254,253,207,56)
- STOR gyuyfotry.avi
- 150 Ok to send data. //Клиент передает содержимое файла
- 226 File receive OK.
- QUIT
- 221 Goodbye.

- Аргумент 192,168,254,253,207,56 означает, что соединение от сервера ожидается на узле с IP-адресом 192.168.254.253 на порту 207*256+56=53048.

- На многих FTP-серверах существует каталог (под названием incoming, upload и т. п.), открытый на запись и предназначенный для закачки файлов на сервер. Это позволяет пользователям наполнять сервер свежими данными.

PASSIVE MODE

- Изначально протокол предполагал встречное TCP-соединение от сервера к клиенту для передачи файла или содержимого каталога. Это делало невозможным общение с сервером, если клиент находится за IP NAT, кроме того, часто запрос соединения к клиенту блокируется файерволом. Чтобы этого избежать, было разработано расширение протокола FTP passive mode, когда соединение для передачи данных тоже происходит от клиента к серверу. Важным моментом является то, что клиент устанавливает соединение с адресом и портом, указанным сервером. Порт сервер выбирает случайным образом из определённого диапазона (49152-65534). Поэтому при нахождении ftp-сервера за NAT, следует явно указать в настройках сервера его адрес.

NAT-PT

- Специально для работы FTP-протокола через межсетевые экраны было сделано расширение NAT, называемое NAT-PT (rfc2766), позволяющее транслировать входящие соединения от сервера к клиенту через NAT. В процессе такого соединения NAT подменяет передаваемые данные от клиента, указывая серверу истинный адрес и порт, с которым сможет соединиться сервер, а потом транслирует соединение от сервера от этого адреса клиенту на его адрес. Несмотря на все меры и нововведения, принятые для поддержки FTP-протокола, на практике функция NAT-PT обычно отключается во всех роутерах и маршрутизаторах с целью обеспечения дополнительной безопасности от вирусных угроз.

FXP

- FXP (англ. File eXchange Protocol — протокол обмена файлами) — способ передачи файлов между двумя FTP-серверами напрямую, не закачивая их на свой компьютер . При FXP-сессии клиент открывает два FTP-соединения к двум разным серверам, запрашивая файл на первом сервере, указывая в команде PORT IP-адрес второго сервера.

- Несомненным преимуществом поддержки стандарта FXP является то, что на конечных пользователей, желающих скопировать файлы с одного FTP-сервера на другой, уже не действует ограничение пропускной способности их собственного интернет-соединения. Нет необходимости скачивать себе файл, чтобы потом положить его на другой FTP-сервер. Таким образом, время передачи файлов будет зависеть только от скорости соединения между двумя удаленными FTP-серверами, которая в большинстве случаев заведомо больше «пользовательской».

FXP

- К сожалению, FXP стал использоваться злоумышленникам для атак на другие серверы: в команде PORT указывается IP-адрес и порт атакуемого сервиса на компьютере жертвы, и командами RETR/STOR производится обращение на этот порт от лица FTP-сервера, а не атакующей машины, что позволяло устраивать масштабные DDoS-атаки с использованием сразу многих FTP-серверов, либо обходить систему безопасности компьютера жертвы, если он полагается только на проверку IP клиента и используемый для атаки FTP-сервер находится в доверенной сети или на шлюзе. В результате сейчас практически все серверы проверяют соответствие IP-адреса, указанного в команде PORT, IP-адресу FTP-клиента и по умолчанию запрещают использование там IP-адресов третьих сторон. Таким образом, использование FXP невозможно при работе с публичными FTP-серверами.

FTP-клиент

- FTP-клиент — программа для упрощения доступа к FTP серверу. В зависимости от назначения может либо предоставлять пользователю простой доступ к удаленному FTP-серверу в режиме текстовой консоли, беря на себя только работу по пересылке команд пользователя и файлов, либо отображать файлы на удаленном сервере как если бы они являлись частью файловой системы компьютера пользователя, либо и то и другое. В последних двух случаях FTP-клиент берет на себя задачу интерпретации действий пользователя в команды протокола FTP, тем самым давая возможность использовать протокол передачи файлов без ознакомления со всеми его премудростями.

FTP-клиент

- Частными примерами использования FTP-клиента могут быть:
- Публикация страниц сайта на интернет-сервере Веб-разработчиком
- Скачивание музыки, программ и любых других файлов данных обычным пользователем интернета. Данный пример зачастую даже не осознается многими пользователями как использование FTP-клиента и протокола, так как многие публичные сервера не запрашивают дополнительных данных для аутентификации пользователей, а Интернет-браузеры (также являющиеся FTP-клиентами) осуществляют скачивание файлов без дополнительных вопросов.

FTP-клиент

- Примерами таких программ могут служить:

- Интернет-браузеры (часто работают в режиме «только чтение», то есть не позволяют добавлять файлы на сервер)
- Многие файловые менеджеры, например: Windows Explorer (Проводник), Total Commander, FAR, Midnight Commander, Krusader
- Специализированные программы, например: FileZilla

Права доступа и авторизация

- Файловая система на удаленном сервере как правило имеет настройки прав доступа для различных пользователей. Так, например, анонимным пользователям могут быть доступны лишь некоторые файлы, о существовании других пользователи знать не будут.
- Другой группе пользователей могут быть доступны другие файлы или, например, в дополнение к правам на чтение файлов, могут быть также даны права на запись новых или обновление имеющихся файлов. Диапазон вариантов прав доступа зависит от операционной системы и программного обеспечения каждого конкретного FTP-сервера. Как правило, разделяют права на просмотр содержимого папки (то есть возможность получить список содержащихся в ней файлов), на чтение файла(ов), на запись (создание, удаление, обновление) файла(ов)

- Для авторизации FTP-сервер, при подключении к нему FTP-клиента, запрашивает у последнего имя пользователя и пароль. Большинство FTP-клиентов в свою очередь запрашивают эти данные у пользователя в интерактивном режиме. Есть также и другой способ указать эти данные, включив их в URL FTP-сервера. Так, например, в строке
- ftp://vasya:key@ftp.example.com
- ftp:// — указание того, что мы используем протокол FTP
- vasya — имя пользователя
- : — разделитель имени пользователя и пароля
- key — пароль
- @ — разделитель аутентификационной информации и адреса сервера
- ftp.example.com — адрес FTP-сервера

Коды ответов FTP

- **Первая позиция**

- Единица означает, что команда принята к выполнению но ещё не завершена
- Двойка означает, что выполнение команды успешно завершено
- Тройка говорит о том, что команда принята и ожидается какая-либо дополнительная команда
- Четверка говорит о том, что в данный момент команда выполнена быть не может
- Пятерка означает принципиальную невозможность выполнения команды

Коды ответов FTP

- **Вторая позиция**

- Ноль соответствует синтаксической ошибке
- Единица соответствует информационному сообщению
- Двойка говорит о том, что сообщение относится либо к управляющему соединению, либо к соединению данных
- Тройка соответствует сообщениям об аутентификации пользователя и его правах
- Значение четверки не определено
- Пятерка соответствует сообщению о состоянии файловой системы

Коды ответов FTP

- **Третья позиция**
- Третья цифра окончательно специфицирует ошибку.

- Все коды см. http://ru.wikipedia.org/wiki/Список_ошибок_FTP_сервера

Демонстрация

- Разные FTP клиенты
- Подключение с помощью telnet