Занятие 18.

Тема: **Сетевое администрирование Linux. Протокол TCP. Занятие второе.**

Вид занятия: лекция, практическое занятие.

Учебные вопросы:

1. FTP. vsftpd.
2. HTTP. Apache.

Время: 90 минут

Литература:

1. Cysco systems и др. - Руководство по технологиям объеденненных сетей, 3-е издание. : Пер. с англ. - М. : Издательский дом “Вильямс”, 2002. - 1040 с. : ил. - парал. тит. англ.

2. Кирх. О, Доусон Т. - Linux для профессионалов. Руководство администратора сети, второе издание. - СПб.: Питер, 2001. - 496 с.; ил.

Ход занятия.

1. Протокол FTP (File Transfer Protocol) – один из старейших в интернет. Это протокол седьмого уровня (уровня приложений) модели OSI, основанный на надежной передаче данных (протоколе TCP, порты 21, 20).

Работа с ftp-ресурсами сходна с работой в локальной файловой системе. Существует множество специализированных клиентов для работы с протоколом FTP. Однако практически все современные браузеры способны обрабатывать информацию с FTP-ресурсов. Их мы и будем использовать в практической части сегодняшнего занятия.

FTP-серверов значительно меньше чем клиентов, но тоже достаточно много, чтобы можно было в них запутаться. Мы с Вами будем настраивать FTP-сервер vsftpd (Very Secure FTP Daemon – очень надежный FTP-демон), входящий в поставку ASPLinux.

Перед рассмотрением его настройки, я хочу немного рассказать о работе протокола FTP. Этот протокол изначально является протоколом с аутентификацией по имени пользователя. Однако для протокола FTP существует и так называемый анонимный режим. В случае его использования (браузеры используют этот режим по умолчанию) вместо имени вводится anonymous, а вместо пароля – адрес электронной почты (браузер использует или настоящий из адресной книги, или случайно подобранный).

Другой особенностью протокола является использование разных режимов – пассивного и активного. В *пассивном* режиме клиент открывает соединения для передачи данных и управляет потоком, а сервер пассивно отдает данные. Этот режим хорошо работает из внутренних сетей с фэйковой адресацией. В *активном* режиме поток для передачи данных открывает и контролирует сервер. Однако, если клиент находится за файрволом с преобразованием адресов (маскарадингом), то он не сможет работать с сервером в этом режиме.

Последней особенностью, обсуждаемой нами, будет передача данных в бинарном или текстовом (ascii) виде. Некоторые бинарные данные в первых версиях серверов/клиентов не могли переданы в прямом виде по сети в связи с особенностями реализации FTP. Для этой цели были придуманы несколько режимов – бинарный, когда передающиеся данные никак не преобразовываются для передачи по сети, и ascii, когда данные с помощью определенного кодирования преобразуются в последовательность символов ascii (с кодами от 0 до 127). Формат ascii увеличивал размер файла, а соответственно и время загрузки из сети, но позволял преодолеть возникающие проблемы. Современные FTP-серверы/клиенты самостоятельно способны выбирать нужный режим передачи, поэтому пользователь в большинстве случаев не задумывается об этом.

Vsftpd представляет из себя программу-демон. В ASPLinux для него предварительно создан скрипт запуска, помещенный в /etc/rc.d/init.d с именем vsftpd. Сам исполняемый файл адресуется как /usr/sbin/vsftpd.

За настройку сервера отвечают несколько файлов:

/etc/vsftpd.busy_banner – файл, в котором записывается сообщение, выдаваемое клиенту, когда сервер не может ответить на запрос.

/etc/vsftpd.ftpusers – содержит список пользователей, которым запрещен доступ по ftp. Как правило этот файл содержит список критически важных для системы пользователей, таких как root, bin, lpd и другие.

/etc/vsftpd.user_list – список пользователей, значение которого меняется в зависимости от того, как установлен параметр userlist_deny в основном файле конфигурации. Если Этот параметр установлен в NO, то на FTP смогут попасть только пользователи, указанные в этом файле, если в YES, то все, кроме этих пользователей. Нужно иметь в виду, что если пользователь запрещен в файле /etc/vsftpd.ftpusers, то он не сможет иметь доступ, даже будучи разрешенным в этом файле.

/etc/vsftpd/vsftpd.conf -основной файл конфигурации сервера. Рассмотрим его поподробнее:

anonymous_enable=YES – параметр-переключатель, разрешающий или запрещающий доступ к анонимному FTP-каталогу (/var/ftp/pub)

local_enable=YES – если этот параметр стоит в NO, то пользователи той же системы, где запущен сервер, не могут получить к нему доступ.

write_enable=YES – Если этот параметр установлен в NO, то ни один из пользователей не имеет права закачать фалы на FTP-ресурс.

local_umask=022 – Определяет права доступа к файлам для всех пользователей, кроме anonymous.

anon_upload_enable=YES – Если параметр установлен в YES, то анонимные пользователи могут изменять существующие в каталоге /var/ftp/pub.

anon_mkdir_write_enable=YES – Позволяет анонимным пользователям закачивать файлы на FTP-ресурс и создавать каталоги.

dirmessage_enable=YES – Если параметр включен, то FTP-сервер будет выдавать сообщение из файла при переходе в каталог. Это сообщение может содержаться в файле с именем .message внутри каталога, однако имя файла может быть дополнительно указано с помощью опции ***message_file***.

xferlog_enable=YES – разрешает серверу записывать журнал с менами переданных файлов. По умолчанию, журнал пишется в /var/log/vsftpd.log, олднако имя фала может быть дополнительно указано опцией ***xferlog_file.*** Формат файла может быть указан сьтандарный (YES) или нестандартный опцией ***xferlog_std_format***.

connect_from_port_20=YES – позволяет использовать для передачи данный 20-й порт.

chown_uploads=YES – изменяет владельца файла, закачанного анонимным пользователем на того, который указан в параметре ***chown_username.***

idle_session_timeout – указывает время в секундах, через которое будет разорвано соединение с клиентом, не выполняющим никаких действий.

data_connection_timeout – указывает время в секундах, через которое будет разорвано соединение в случае перерыва в передаче данных.

Дополнительную информацию по конфигурации этого сервера можно получить в руководстве man (страницы vsftpd, vsftpd.conf).

2. Протокол HTTP – на сегодняшний день самый распространенный протокол интернет, базирующийся на TCP (порт 80). Множество смежный стандартов, связанных с публикацией, обработкой и отображение HTML-страниц, настолько усложнили вэб-серверы, что их конфигурации подчас является непростым делом для начинающего администратора. Мы с вами попробуем настроить сервер на базовую работу и посмотреть основные параметры его конфигурации.

В качестве пособия мы будем использовать один из самых мощнейших и самый распространенный в интернет сервер Apache в версии 2.0.40. Конфигурирование Apache 2.x сильно отличается от конфигурирования его предшественника – линейки 1.3

Основным файлом конфигурации является httpd.conf, который в RedHat-совместимых системах (в том числе в ASPLinux) расположен в /etc/httpd/conf.

ServerTokens OS – этот параметр позволяет скрыть информацию об используемых модулях.

ServerRoot "/etc/httpd" – указывает на каталог, где расположены конфмгурационные файлы, файлы журналов и другая необходимая информация для работы сервера.

Timeout 300 – указывает время в секундах, через которое будет разорвано соединение с клиентом, не проявляющим активности.

KeepAlive Off – разрешает или запрещает поддерживать соединие с клиентом пакетами

типа PING-PONG.

Listen 80 – указывает порт (или ip-адрес и порт в формате 192.168.2.2:80) на котром будет функционировать вэб-сервер.

LoadModule – позволяет загрузить и использовать модуль расширения для поддержки дополнительных возможностей у сервера.

User apache, Group apache – параметры указывают пользователя и группу, от имени которого должен будет работать сервер.

ServerAdmin root@localhost – указывает адрес электронной почты администратора сервера, который будет указан на страницах с сообщениями об ошибках.

ServerName hosters.volnet.ru – указывает доменное имя, с которым работает сервер. Если для компьютера доменное имя не определено, с эту позицию вписывается IP-адрес.

DocumentRoot "/var/www/html" – указывает каталог, в котором располагаются документы HTML.

Раздел Directory описывает каталог, в котором расположены документы.

<Directory "/var/www/html"> -начало описания

Options – опции каталога с документами, указываемые через пробел. В качестве опций могут использоваться: *Includes* – включаемый файлы, *FollowSymLinks* – переход по символьным ссылкам, *SymLinksifOwnerMatch* – переход по символьны ссылкам, если владелец совпадает, *ExecCGI* – выполнять файлы CGI и передавать вывод файлов клиенту и другие.

AllowOverride - позволяет изменять параметры вложенных директорий с помощью файлов .htaccess полностью (All), не изменять (None) или отдельные параметры.

Order – определяет допустимые значения при конфигурации безопасности. Может включать параметры Deny, Allow или то и другое через запятую.

Deny/Allow from all/192.168.3.11 – определяет доступ к каталогу.

</Directory> - закрывает описание каталога.