Взято: http://www.lissyara.su/articles/freebsd/programms/vsftpd+ad_vsftpd+mysql/

Автор: atrium .

Здравствуйте уважаемые читатели!
Сегодня попробуем разобраться с прекрасным ftp сервером - VSFTPD (Официальный сайт). Но для начала некоторые общие понятия :).

FTP – это протокол передачи файлов. Программы, использующие этот протокол, стали частью отдельного сервиса Интернет. Для пользования FTP нужна специальная программа – FTP-клиент. FTP-клиент - это сервисная программа, с помощью которой можно произвести соединение с FTP сервером. Обычно эта программа имеет командную строку, но некоторые имеют оконный интерфейс и не требуют запоминания команд. Пример FTP-клиента - программы CuteFTP, Go!Zilla, ReGet и т.д, называются они менеджерами загрузки. У них удобный интерфейс и позволяют пользователям удобно осуществлять загрузку-выгрузку файлов.

FTP-сервер - компьютер, который содержит общедоступные файлы и настроен на поддержку протокола FTP (FTP-сервер должен иметь программное обеспечение, поддерживающее протокол FTP).

И так приступим к настройке нашего FTP сервера, вся установка проводилась на FreeBSD v_7.1. Нам понадобятся следующие пакеты:

Port: vsftpd-**2**.**0**.
Path: /usr/ports/ftp/vsftpd
Info: A FTP daemon that aims to be "ver

Port: mysql-server-**5**.**0**.67_1
Path: /usr/ports/databases/mysql50-server
Info: Multithreaded SQL database (server)

Port: pam_mysql-**0**.**7**.r1
Path: /usr/ports/security/pam-mysql

Info: A pam module for authenticating with MySQL

Так же для связки FTP с AD необходимо что бы машина с FreeBSD была включена в домен Windows. Статья, которая описывает процедуру введения машины с FreeBSD в домен - FreeBSD и AD .

Устанавливаем базу данных MySQL, пример настройки и установки я не буду приводить, думаю в интернете есть большое количество статей :)

Настроим сначала связку vsftpd и AD, для этого устанавливаем vsftpd со следующими опциями:

```
[X] RC_NG          install          RC_NG script
[X] VSFTPD_SSL     Include ssl support   SSL
```

После того как vsftpd установлен, необходимо создать пользователя 'ftp' с домешнем каталогом, в который будут логиниться anonymous и создать файл конфигурации в каталоге /usr/local/etc есть файл vsftpd.conf.dist, его можно переименовать в vsftpd.conf, но лучше сделать с нуля:

```
touch                /usr/local/etc/vsftpd.conf
```

После создания файла vsftpd.conf приступаем к внесению конфигурационных опций :) Созданный нами конфиг предполагает работу vsftpd в качестве анонимного сервера и сервера с авторизацией юзеров из AD. По желанию можно отключить одно из двух :)

```
# Работа сервера в standalone режиме
listen=              YES

# Работа в качестве демона
background=          YES

# На каком IP работать
```

listen_address= **192** . **168** .

# Имя файла pam сервиса в /etc/pam.d
pam_service_name= ftp
session_support= YES

# Включить пассивный режим
pasv_enable= YES
pasv_max_port= **50000**
pasv_min_port= **60000**

# Использовать sendfile
use_sendfile= YES

# Для пролхих клиентов
async_abor_enable= YES

#----Ограничения
#---
# Определяет какие email адреса использовать для анонимов в качестве пароля
# из файла email_password_file
secure_email_list_enable= NO
#email_password_file=/usr/local/etc/vsftpd_email.password

# Запретить использовать email для доступа анонима из файла banned_email_file
deny_email_enable= NO
#banned_email_file=/usr/local/etc/vsftpd_email.deny

# Chroot в каталог
secure_chroot_dir=/usr/local/share/vsftpd/empty

# Chroot по списку из файла chroot_list_file
chroot_list_enable= NO
#chroot_list_file=/usr/local/etc/vsftpd_chroot.list

# Разрешить запись
write_enable= YES

# Чтение юзеров из файлов deny
userlist_enable= YES

# Запрещён доступ для юзеров перечисленных в указанном файле
userlist_deny= YES
userlist_file=/usr/local/etc/vsftpd_user.

```
# Время ожидания соединения на порт в sec
connect_timeout=        60

# Время передачи простоя, если данные не передаются
data_connection_timeout=300

# Задержка перед сообщением об ошибке регистрации
delay_failed_login=     1

# Задержка при правильной регистрации
delay_successful_login=0

# Задрежка между вводом FTP команд в sec
idle_session_timeout=   300

# Запрет команды chmod
chmod_enable=           NO

# Максимальное количество клиентов
max_clients=            10

# Максимально количество неправильных входов, далее разрыв
max_login_fails=        3

# Максимальное количество соединений с одного ip
max_per_ip=             1

# Запрещённые файлы через запятую
deny_file={*.lnk}

# Скрыть указанные файлы через запятую
hide_file={*.lnk}

# Запретить использовать команду ls -R
ls_recurse_enable=      NO

# Проверка существования shell в /etc/shells
check_shell=            NO

# Не показывать файлы начинающиеся с точки
force_dot_files=        NO

# Скрывать кто является реальным владельцем файла
# Будет указываться владелец 'ftp'
hide_ids=               YES
```

```
# Блокировать доступ к загружаемому файлу
lock_upload_files=        YES

# Разрешить чтение каталогов
dirlist_enable=           YES

# Разрешить загрузку
download_enable=          YES

# Удалить файлы загруженные с ошибками или недокачанные
delete_failed_uploads= YES

# Разрешить соединение на 20 порт
connect_from_port_20=NO
#-----------------------------------------------



#----Локальные пользователи
#-----------------------------------------------
# Разрешить локальных пользователей из файла /etc/passwd
local_enable=             YES

# Использовать привелегии локальных юзеров для виртуальных
# Если NO то используются привелегии anonymous
virtual_use_local_privs=YES

# Посадить в тюрьму локального юзера
chroot_local_user=        YES

# Маска для локальных пользователей
local_umask=              022

# Каталог для локальных юзеров
local_root=/home/IMPEX/$USER

# Создание папки пользователя
# Образец каталога берётся из параметра guest_username
user_sub_token=           $USER

# Chroot в каталоге юзера указанного в /etc/passwd
passwd_chroot_enable=YES

# Скорость закачки byt/sec
local_max_rate=           2097152
#-----------------------------------------------
```

```
#----Анонимные пользователи
#-----------------------------------------------
# Разрешить анонимных пользователей
anonymous_enable=     YES

# Каталог для анонимов
anon_root=/server/ftp

# Разрешает загрузку. Работает при write_enable=YES
anon_upload_enable=   YES

# Создание каталогов. Работает при write_enable=YES
anon_mkdir_write_enable=YES

# Создание, загрузка и удаление
anon_other_write_enable=NO

# Не использовать пароль для анонимного доступа
no_anon_password=     YES

# Маска для файлов созаваемых анонимом
anon_umask=           022

# Режим для загружаемых файлов
chown_upload_mode=    0440

# Только чтение, запрещает скачивать файлы с FTP
anon_world_readable_only=NO

# Установить владельцем файлов юзера указанного в chown_username
chown_uploads=        YES
chown_username=       ftp

# Скорость закачки byt/sec
anon_max_rate=        2097152
#-----------------------------------------------



#----Ведение логов
#-----------------------------------------------
# Логирование всех запросов к ftp
# Работает при выключенной опции xferlog_std_format
# Используется для отладки
log_ftp_protocol=     NO
```

```
# Файл логов
vsftpd_log_file=/var/log/vsftpd.log

# Отправка логов в syslog
syslog_enable=          YES

# Паралельное ведение логов в vsftpd.log и xferlog
dual_log_enable=        NO

# Логи детальной upload/download
xferlog_enable=         NO
xferlog_file=/var/log/vsftpd.log
xferlog_std_format=     YES
#-----------------------------------------------


#----Определение кодировки
#-----------------------------------------------
# Использование ASCII  при скачке/загрузке
# Работают русские символы, кодировка для клиента KOI8-R
ascii_download_enable=YES
ascii_upload_enable=    YES
#-----------------------------------------------



#----Сообщения
#-----------------------------------------------
# Банер приветствия при входе
ftpd_banner=Welcom    to                FTP                service

# Показ сообщения пользователю из файла '.message' при входе в каталог. Файл определяется
# в опции message_file. Файл должен находится в этом же каталоге.
dirmessage_enable=      NO
message_file=.          message
#-----------------------------------------------


# Разрешить гостя. Все не анонимные пользователи логинятся как гость
# Имя юзера гостя определено в опции 'guest_username'
guest_enable=           NO
guest_username=atrium

# Пользователь для анонимных юзеров
ftp_username=           ftp
nopriv_user=nobody
```

```
# Показать имя и группу вместо uid/gid
text_userdb_names=     YES
```

После того как настроили vsftpd, создаём файл с именем 'ftp' в /etc/pam.d, если он отсутствует, со следующим содержанием:

```
auth    required  pam_nologin.so  no_warn
auth    sufficient  /usr/local/lib/pam_winbind.so krb5_auth
auth    sufficient  pam_opie.so no_fake_prompts
auth    requisite pam_opieaccess.so    allow_local no_warn
auth    required  pam_unix.so no_warn try_first_pass

account   required  pam_nologin.so  no_warn
account   sufficient  /usr/local/lib/pam_winbind.so krb5_auth
account   required  pam_unix.so

session   required  pam_permit.so
```

Делаем проверку:

```
220                    Welcom              to                  FTP                 service
Name                   (                   10                  .                   178
331                    Please specify the password.
Password:
230                    Login               successful.
Remote system type is UNIX.
Using binary mode      to                  transfer files.
```

Настроим теперь vsftpd с MySQL :)
Как говорилось выше, базу данных MySQL установили и запустили, всё работает. Создаём необходимую базу и таблицу, в которой будут храниться наши юзвери :)

```
--                      MySQL                   dump                    10                      .
--
--                      Host                    :                       localhost                   Datal
-- ------------------------------------------------------
-- Server version       5                       .                       0                       .

/*!40101                SET                     @OLD_CHARACTER_SET_CLIENT=@@CHARACTE
/*!40101                SET                     @OLD_CHARACTER_SET_RESULTS=@@CHARAC
/*!40101                SET                     @OLD_COLLATION_CONNECTION=@@COLLATIO
/*!40101                SET                     NAMES utf8 */;
/*!40103                SET                     @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103                SET                     TIME_ZONE='+            00                      :
/*!40014                SET                     @OLD_UNIQUE_CHE0KS=@@UNIQUE_CHE?KS, U
/*!40014                SET                     @OLD_FOREIGN_KE0_CHECKS=@@FOREIGN_KE?N_KE
/*!40101                SET                     @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='
/*!40111                SET                     @OLD_SQL_NOTES=@@SQL_NOTES, SQL_N?TES

--
-- Current Database: `vsftpd`
--

CREATE                  DATABASE /*!32312       IF                      NOT                     EXISTS
                /*!40100       DEFAULT                 CHARACTER               SET                     cp1251

USE `vsftpd`;

--
-- Table structure      for                     table `accounts`
--

DROP                    TABLE                   IF                      EXISTS `accounts`;
SET                     @saved_cs_client    = @@character_set_client;
SET                     character_set_client = utf8;
CREATE                  TABLE `accounts` (
  `id` int(             11                      )                       NOT                     NULL a
  `username` varchar(   50                      )                       NOT                     NULL,
  `pass` varchar(       50                      )                       NOT                     NULL,
  PRIMARY KEY  (`id`),
  UNIQUE KEY `username` (`username`)
) ENGINE=MyISAM     DEFAULT                 CHARSET=cp1251;
SET                     character_set_client = @saved_cs_client;
```

Создадим тестового пользователя, пароль будет шифроваться алгоритмом MD5, заданный алгоритм определят параметр crypt=3 в файле /etc/pam.d/ftp, листинг которого

приводится ниже:

```
use vsftpd;
insert into accounts set userna
```

После создания базы, таблицы и пользователя необходимо установить pam-mysql и создать файл с именем 'ftp' в каталоге /etc/pam.d, если он отсутствует, со следующим содержанием:

```
auth requisite user/usr/local/lib/pam_mysql.so passwd=root \
db=vsftpd host = localhost table=a
account requisite user/usr/local/lib/pam_mysql.so passwd=root \
db=vsftpd host = localhost table=a
```

После всех операций в конфиге **vsftpd.conf**, который был представлен выше необходимо изменить:

```
# Разрешить гостя. Все не анонимные пользователи логинятся как гость
# Имя юзера гостя определено в опции 'guest_username'
guest_enable= YES
guest_username= ftp
```

Делаем проверку:

```
220 Welcom to FTP service
Name ( 10 . 178
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Важно:
- Для доступа к MySQL создайте отдельного пользователя с минимальными привилегиями
- Представленный конфиг vsftpd.conf подходит также для работы с локальными пользователями, аутентификация определяется с помощью pam.

atrium, 2009-06-01 в 15:35:41

Спасибо за наводку, совсем забыл про этот модуль :)

session required /usr/local/lib/pam_mkhomedir.so debug mode=750 skel=/usr/share/skel

И всё работает к существующим pam конфигурациям