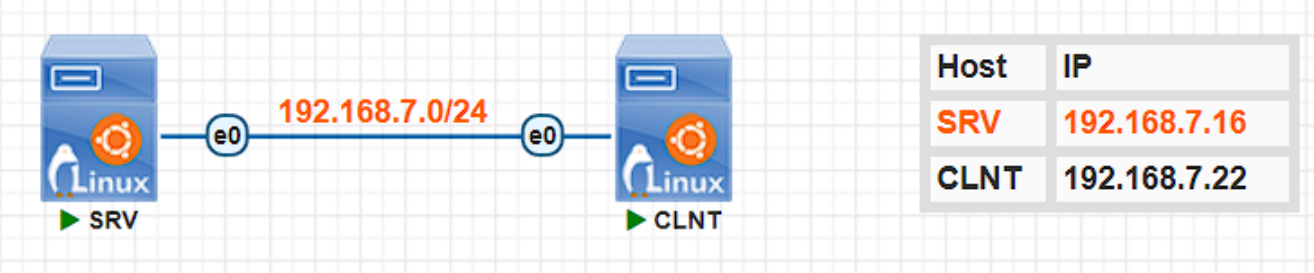
13-PR-FTP

Топология



Host	IP
SRV	192.168.7.16
CLNT	192.168.7.22

Задание

Базовая настройка

1. Настройте имена устройств в соответствии с топологией
2. Настройте часовой пояс Алматы
3. Настройте адреса в соответствии с топологией

```
hostnamectl set-hostname SRV,CLNT
timedatectl set-timezone Asia/Almaty
#SRV
vi /etc/network/interfaces

auto ens4
iface ens4 inet static
        address 192.168.7.16/24
#CLNT
auto ens4
iface ens4 inet static
        address 192.168.7.22/24
        gateway 192.168.7.22
```

Доступ в домашний каталог пользователя

Установка службы

Установите службу `vsftpd` на SRV

Настройка службы

1. Откройте основной конфигурационный файл **vsftpd**: `vi /etc/vsftpd.conf`
2. Удалите комментарии командой: `:g/^[#\n]/d`
3. Приведите конфиг к следующему виду:

```
#listen=NO
listen_ipv6=YES
anonymous_enable=NO
local_enable=YES
#dirmessage_enable=YES
#use_localtime=YES
#xferlog_enable=YES
connect_from_port_20=YES
secure_chroot_dir=/var/run/vsftpd/empty
pam_service_name=vsftpd
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
#ssl_enable=NO
```

4. Перезагрузите службу: `vsftpd`
   Значение параметров:

- `listen` - отвечает за прослушивание службой vsftpd IPv4 сокета
- `listen_ipv6` - отвечает за прослушивание службой vsftpd IPv6 и IPv4 сокета
  - В конфиге по умолчанию, vsftpd слушает и IPv4 и IPv6 трафик
- `anonymous_enable` - определяет доступ анонимным пользователям к серверу
- `local_enable` - использование локальной базы пользователей
- `dirmessage_enable` - определяет будет ли отображаться пользователю сообщение при первом открытии каталога
  - по умолчанию ищется файл `.message`, но можно переопределить параметром: `message_file`
- `use_localtime` - должен ли vsftpd отображать время с учетом вашего часового пояса или показывать время по GMT
- `xferlog_enable` - сохранять ли в логах подробное описание загрузок
  - по умолчанию будут писаться в файл: `/var/log/vsftpd.log`
- `connect_from_port_20` - использовать 20 порт для передачи данных или нет
- `secure_chroot_dir` - имя пустого каталога, без прав записи для пользователя ftp, используется в качестве защищенной тюрьмы chroot() в тех случаях, когда vsftpd не требует доступа к файловой системе.
- `pam_service_name` - определяет имя службы PAM, которую будет использовать vsftpd.

- `ssl_enable` - включает поддержку шифрованного подключения
- `rsa_cert_file` - путь до файла открытого ключа сертификата сервера
- `rsa_private_key_file` - путь до файла закрытого ключа сертификата сервера

Информация о пользователях

Служба vsftpd в нашей настройке использует системную базу пользователей. Ознакомиться со списком пользователей мы можем открыв файл: `/etc/passwd`
Изучим вывод на примере пользователя **user**:

```
user:x:1000:1000:user,,,:/home/user:/bin/bash
```

Нам доступна следующая информация (читаем слева на право):

- **user** - имя пользователя
- **x** - раньше тут был пароль в шифрованном виде, теперь просто пропуск
- **1000** - uid - user id - id пользователя
- **1000** - gid - group id - id группы пользователя
- **user,,,** - поле для комментариев об учетной записи
- **/home/user** - путь до домашнего каталога пользователя
- **/bin/bash** - командная оболочка по умолчанию

Создание пользователя

1. Создадим пользователя под которым будем входить в систему используя команду: `useradd test1`
2. Изучим что записалось в passwd: `cat /etc/passwd`

```
test1:x:1001:1001::/home/test1:/bin/sh
```

3. Если вы сделали что то не так, то удалить пользователя вы можете командой: `userdel user_name`
4. Видим что по умолчанию `useradd`:
   2. продлевает uid и gid от предыдущего
   3. размещает домашний каталог пользователя в `/home/`
   4. оболочка назначена: `/bin/sh`
   5. для пользователей которые будут работать в консоли лучше установить `/bin/bash`, но в нашем случае это не критично
5. Посмотрим создался ли домашний каталог: `ls /home`

```
root@SRV:~# ls /home/
user
```

6. А тут только лишь пользователь **user**
7. Создадим домашний каталог: `mkdir /home/test1`
    1. И файл в нем с вашей фамилией: `touch /home/test1/ivanov.txt`
8. Сравним права доступа к каталогам test1 и user: `ls -l /home`

```
root@SRV:~# ls -l /home
total 8
drwxr-xr-x 2 root root 4096 Feb 24 10:21 test1
drwx------ 2 user user 4096 Nov 10 03:22 user
```

Права доступа в linux

Рассмотрим вывод для каталога **test1**:

1. **drwxr-xr-x**:
    1. **d** - говорит о том что это каталог, у файлов там будет **-**
    2. **rwxr-xr-x** - три группы прав:
        1. **rwx** - права владельца каталога
        2. **r-x** - права группы владеющей каталогом
        3. **r-x** - права для всех прочих пользователей
    3. **root root** - владелец каталога пользователь **root**, группа - **root**
    4. Если владелец сопоставляет нас с одним пользователем системы, то параметр группы позволяет дать специальные права конкретной группе пользователей
    4. **4096** - "размер" каталога, в случае с каталогами, обычно равна размеру блока файловой системы
    5. **Feb 24 10:21 24 10:21** - дата последнего изменения
    6. **test1** - название каталога

Права имеют несколько вариантов описания:

Буква	Цифра		Значение
r	4	**r**ead	чтение
w	2	**w**rite	запись
x	1	e**x**ecute	выполнение

При указании прав в числовом виде, достаточно использовать три цифры (по одной для владельца, группы и других) которые представляют сумму цифровых значений прав. Например:

- 7 - rwx (4+2+1)
- 6 - rw- (4+2)
- 4 - r-- (4)

Установим верные права доступа к домашнему каталогу

1. По умолчанию доступ к домашнему каталогу разрешается только пользователю владельцу этого каталога
    1. Значит права будут выглядеть либо так: `rwx------` , либо так: `700`
    2. Установим их для каталога **test1**: `chmod -R 700 /home/test1`
        1. Ключ `-R` говорит о том, что измения должны коснуться и всех вложенных файлов и каталогов
2. Так как мы создавали каталог вручную, он получил владельцем нашего пользователя. А нам нужно установить uid и gid пользователя test1 (да это test1 и test1)
    1. Изменим владельца и группу каталога **test1**: `chown -R test1:test1 /home/test1`
        1. Ключ `-R` говорит о том, что измения должны коснуться и всех вложенных файлов и каталогов
3. Посмотрим права на каталоги `ls -l /home` :

```
root@SRV:/home# ls -l
total 12
drwx------ 2 test1 test1 4096 Feb 24 10:21 test1
drwx------ 2 user  user  4096 Nov 10 03:22 user
```

4. Видим теперь, что права на каталог test1 и user идентичны. Значит мы все сделали правильно.

Установка пароля пользователя

1. Мы создали пользователя **test1**, но не указали ему пароль
2. Проверим так ли это: `cat /etc/shadow`

```
user:$y$j9T$RMx5QE0tun5Zj5iH7YJgJ.$G.O2tI62VS9DsZmmJeREH92L1dz8WjI1te7rgLPjbm8
:19671:0:99999:7:::
```

```
test1:!:19777:0:99999:7:::
```

3. Длинная запись у **user** как раз и представляет собой шифр хеша пароля и у **test1** его действительно нет
    1. Установим его командой: `passwd test1`
    2. Проверьте что он установился командой: `cat /etc/shadow`

Подключение с клиента

1. Войдите в систему используя графический интерфейс:
    1. Откройте файловый менеджер
    2. И в адресную строку введите: `ftp://test1@192.168.7.16`
    3. Введите пароль
    4. Вы должны увидеть ранее созданный нами файл

1. Попробуйте изменить файл
    1. Мы получили такой результат по причине того что, при удаленном доступе к каталогу необходимо учитывать настройки доступа как файловой системы так и самой службы
    2. Так мы имеем права на запись в настройках файловой системы, но не имеем их в настройках службы vsftpd
2. Введите новый путь: `ftp://test1@192.168.7.16/`
3. Что мы видим?
    1. По умолчанию ftp по умолчанию открывает наш домашний, но не ограничивает нас только им, и мы можем отправиться в путешествие по нашей же файловой системе

Ограничение пользователя в домашнем каталоге и настройка прав записи

Настройка службы

1. В файл настроек **vsftpd** добавим следующее:
    1. Не переписывайте комментарии!

```
# Авторизированные пользователи монтируются в свои домашние каталоги
chroot_local_user=YES
# Разрешаем пользователям вести запись в домашние каталоги
allow_writeable_chroot=YES
```

```
# Разрешаем запись на сервер
write_enable=YES
```

2. Перезагрузим службу **vsftpd**
    1. Проверьте её статус, что бы убедиться что она запустилась без ошибок
        1. Это важно, так как зачастую при рестарте ошибка может не отобразиться, а сама в логах служба выдаст ошибку и демон не запуститься

```
systemctl restart vsftpd.service
systemctl status vsftpd.service
```

Подключение с клиента

1. Для обновления страница выключите dolphine и включите снова
    1. Попробуйте изменить созданный вами ранее файл.
        1. Успешно?
    2. Попробуйте перейти по пути: `ftp://test1@192.168.7.16/`
        1. Что открылось?

Доступ нескольким пользователям к одному каталогу

Создание пользователя

1. Создайте нового пользователя с именем **test2** и укажите ему домашний каталог `/home/test1`
    1. Используйте команду: `useradd test2 -d /home/test1`
    2. Установите пароль

Настройка прав

1. Создайте группу **testers** командой: `groupadd testers`
2. Добавьте пользователей **test1** и **test2** в группу **testers**:

```
usermod -G testers test1
usermod -G testers test2
```

3. Изменим права на каталог:

```
# Тут пропустили указание пользователя, полскольку его мы менять не планируем
chown :testers /home/test1
```

```
# Добавим права для группы
chmod 770 /home/test1
```

4. Мы не вносили никаких изменений в работу службы FTP, поэтому нет необходимости её перезагружать

Подключение с клиента

1. Откройте путь: `ftp://test2@192.168.7.16`
    1. Введите пароль от пользователя **test2**
    2. В какой каталог вы попали?
    3. Попробуйте создать в нём файл

Доступ для анонимных пользователей к каталогу

Создание каталога и настройка прав

1. Создайте каталог: `opt/public`
    1. Создайте в нем файл `cs1.6.exe`

Настройка службы

1. Добавьте или измените следующие строки в файле настроек **vsftpd**:

```
# Разрешаем доступ к серверу анонимным пользователям
anonymous_enable=YES
# Монтируем анонимных пользователей в каталог /public
anon_root=/opt/public
```

2. Перезагрузите службу **vsftpd** и проверьте её статус

Подключение с клиента

1. Откройте путь: `ftp://anonymous@192.168.7.16`
    1. Выберите вход без пароля
    2. Попробуйте скопировать файл `cs1.6.exe` на рабочий стол
        1. Успешно?