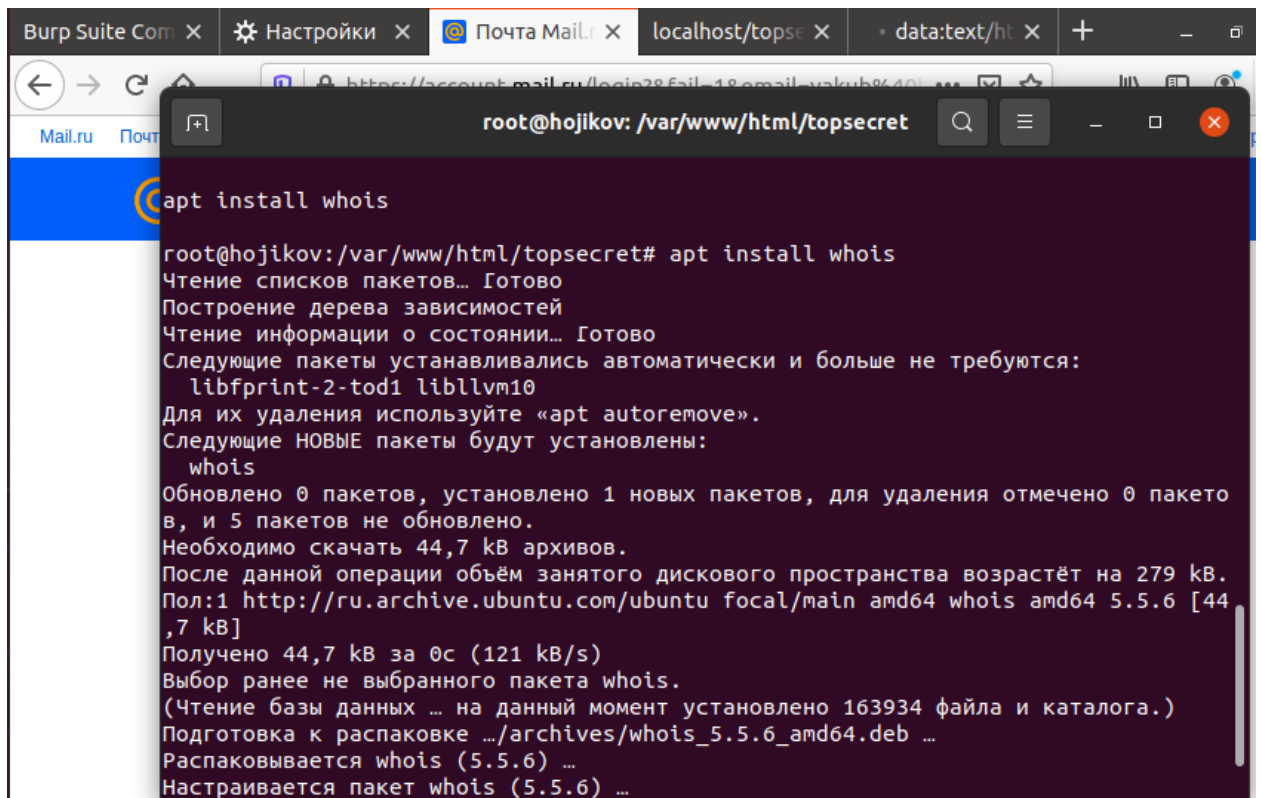
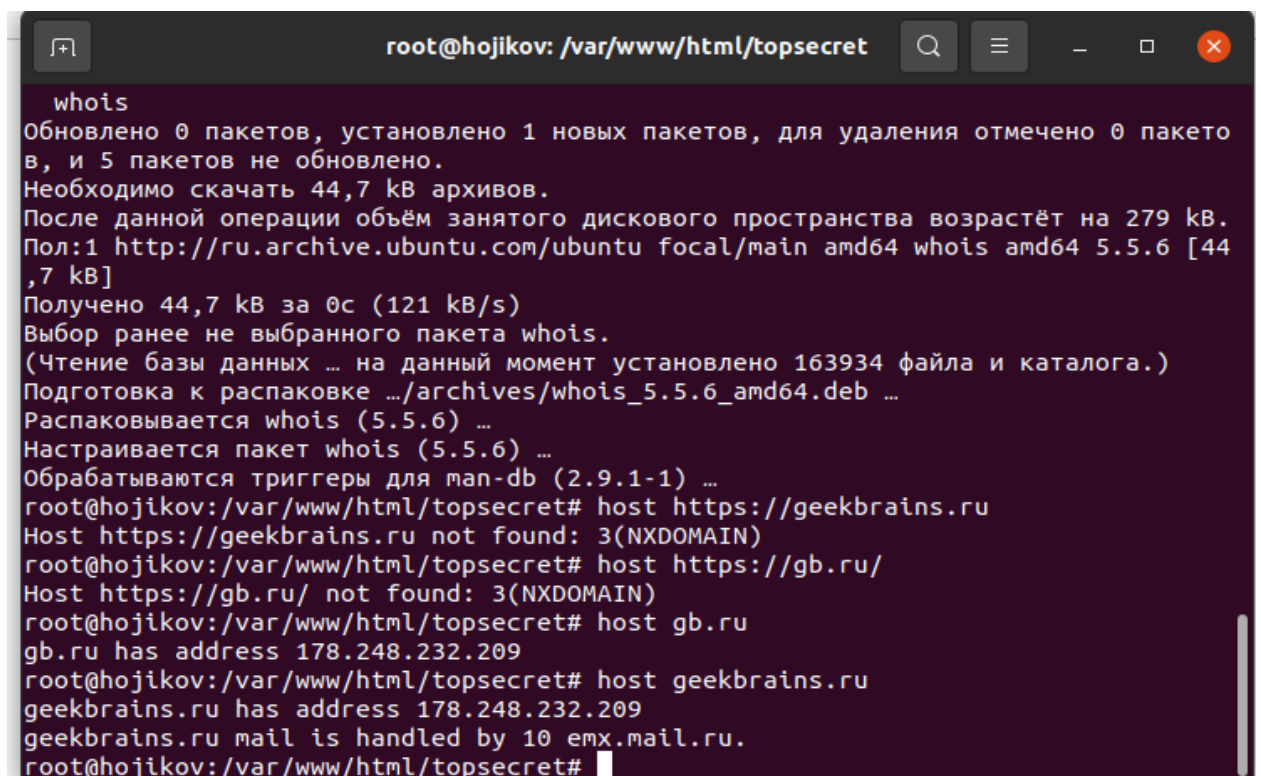


1.Открыть терминал. Установить программы host и whois (если уже не установлены). Выяснить IP адрес сайта <https://geekbrains.ru>. Выяснить IP адрес <http://localhost>.

A screenshot of a terminal window titled 'root@hojikov: /var/www/html/topsecret'. The terminal shows the command 'apt install whois' being executed. The output indicates that the package 'whois' is being installed, with a size of 44.7 kB. The terminal also shows the command 'apt autoremove' being executed, which removes the package 'whois'. The terminal output is as follows:

```
apt install whois
root@hojikov:/var/www/html/topsecret# apt install whois
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  libfprint-2-tod1 libllvm10
Для их удаления используйте «apt autoremove».
Следующие НОВЫЕ пакеты будут установлены:
  whois
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов,
и 5 пакетов не обновлено.
Необходимо скачать 44,7 kB архивов.
После данной операции объем занятого дискового пространства возрастет на 279 kB.
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 whois amd64 5.5.6 [44,7 kB]
Получено 44,7 kB за 0с (121 kB/s)
Выбор ранее не выбранного пакета whois.
(Чтение базы данных ... на данный момент установлено 163934 файла и каталога.)
Подготовка к распаковке .../archives/whois_5.5.6_amd64.deb ...
Распаковывается whois (5.5.6) ...
Настраивается пакет whois (5.5.6) ...
```

Рис1 Установка whois, HOST предустановлен!

A screenshot of a terminal window titled 'root@hojikov: /var/www/html/topsecret'. The terminal shows the command 'whois' being executed, which outputs the IP address of the website 'geekbrains.ru' as 178.248.232.209. The terminal also shows the command 'host https://geekbrains.ru' being executed, which outputs 'Host https://geekbrains.ru not found: 3(NXDOMAIN)'. The terminal output is as follows:

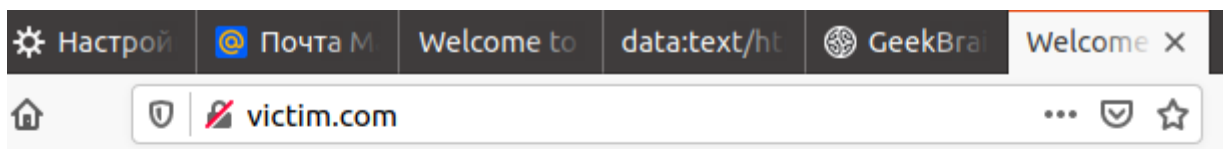
```
whois
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов,
и 5 пакетов не обновлено.
Необходимо скачать 44,7 kB архивов.
После данной операции объем занятого дискового пространства возрастет на 279 kB.
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 whois amd64 5.5.6 [44,7 kB]
Получено 44,7 kB за 0с (121 kB/s)
Выбор ранее не выбранного пакета whois.
(Чтение базы данных ... на данный момент установлено 163934 файла и каталога.)
Подготовка к распаковке .../archives/whois_5.5.6_amd64.deb ...
Распаковывается whois (5.5.6) ...
Настраивается пакет whois (5.5.6) ...
Обрабатываются триггеры для man-db (2.9.1-1) ...
root@hojikov:/var/www/html/topsecret# host https://geekbrains.ru
Host https://geekbrains.ru not found: 3(NXDOMAIN)
root@hojikov:/var/www/html/topsecret# host https://gb.ru/
Host https://gb.ru/ not found: 3(NXDOMAIN)
root@hojikov:/var/www/html/topsecret# host gb.ru
gb.ru has address 178.248.232.209
root@hojikov:/var/www/html/topsecret# host geekbrains.ru
geekbrains.ru has address 178.248.232.209
geekbrains.ru mail is handled by 10 emx.mail.ru.
root@hojikov:/var/www/html/topsecret#
```

Рис.2 Как видно на скрине по указанному адресу(со схемой) хост не работает, только без схемы!

```
root@hojikov: /var/www/html/topsecret
Получено 44,7 kB за 0с (121 kB/s)
Выбор ранее не выбранного пакета whois.
(Чтение базы данных ... на данный момент установлено 163934 файла и каталога.)
Подготовка к распаковке .../archives/whois_5.5.6_amd64.deb ...
Распаковывается whois (5.5.6) ...
Настраивается пакет whois (5.5.6) ...
Обрабатываются триггеры для man-db (2.9.1-1) ...
root@hojikov:/var/www/html/topsecret# host https://geekbrains.ru
Host https://geekbrains.ru not found: 3(NXDOMAIN)
root@hojikov:/var/www/html/topsecret# host https://gb.ru/
Host https://gb.ru/ not found: 3(NXDOMAIN)
root@hojikov:/var/www/html/topsecret# host gb.ru
gb.ru has address 178.248.232.209
root@hojikov:/var/www/html/topsecret# host geekbrains.ru
geekbrains.ru has address 178.248.232.209
geekbrains.ru mail is handled by 10 emx.mail.ru.
root@hojikov:/var/www/html/topsecret# host http://localhost.
Host http://localhost not found: 2(SERVFAIL)
root@hojikov:/var/www/html/topsecret# host http://localhost
Host http://localhost not found: 2(SERVFAIL)
root@hojikov:/var/www/html/topsecret# host localhost
localhost has address 127.0.0.1
localhost has IPv6 address ::1
root@hojikov:/var/www/html/topsecret#
```

Рис.3 Аналогично и для указанного адреса localhost!

2. Найти файл hosts на своем компьютере (виртуальной машине). Сделать так, чтобы адрес сайта <http://attacker.com> и <http://victim.com> соответствовал адрес <http://localhost>.



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Рис.4 Содержимое страницы по адресу <http://victim.com> соответствует содержимому страницы <http://localhost>.

А вот такая же операция с сайтом <http://attacker.com> удалась только на браузере Chromium, Firefox «тупил»...



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

Рис.5 Содержимое страницы по адресу <http://attacker.com> соответствует содержимому страницы <http://localhost>.

3. Запустите nginx и создайте в корневом каталоге директорию blog, а в директории blog создайте файл post.txt. Составьте полный URL (со схемой http или https) к этому файлу и запросите его через браузер.

```
root@hojikov: /var/www
BurpSuiteCommunity Видео Загрузки Музыка 'Рабочий стол'
snar Документы Изображения Общедоступные Шаблоны
root@hojikov:/home/hojikov# cd Документы
root@hojikov:/home/hojikov/Документы# cat > login_password.txt
^Z
[1]+  Остановлен  cat > login_password.txt
root@hojikov:/home/hojikov/Документы# echo > login_password.txt
root@hojikov:/home/hojikov/Документы# nano login_password.txt

Используйте «fg» для возврата в nano

[2]+  Остановлен  nano login_password.txt
root@hojikov:/home/hojikov/Документы# cd /home/hojikov
root@hojikov:/home/hojikov# nano /etc/nginx/sites-available/test.conf

Используйте «fg» для возврата в nano

[3]+  Остановлен  nano /etc/nginx/sites-available/test.conf
root@hojikov:/home/hojikov# nginx -s reload
root@hojikov:/home/hojikov# nginx -s reload
root@hojikov:/home/hojikov# cd /var/www/html
root@hojikov:/var/www/html# mkdir blog
```

Рис.6 Создание директории blog в корневом(/var/www/html) каталоге

```
root@hojikov: /var/www/html/blog

command 'vlog' from deb atfs (1.4pl6-14)
command 'elog' from deb elog (3.1.3-1-1build1)
command 'klog' from deb klog (0.9.8.1-1.1build1)
command 'klog' from deb openafs-krb5 (1.8.4~pre1-1ubuntu2.1)
command 'clog' from deb clog (1.3.0-1build1)
command 'rlog' from deb rcs (5.9.4-6)
command 'flog' from deb flog (1.8+orig-2)
command 'xlog' from deb xlog (2.0.17-2)
command 'plog' from deb ppp (2.4.7-2+4.1ubuntu5.1)

Try: apt install <deb name>

root@hojikov:/var/www/html# cd blog
root@hojikov:/var/www/html/blog# nano post.txt

Используйте «fg» для возврата в nano

[4]+ Остановлен nano post.txt
root@hojikov:/var/www/html/blog# fg
nano post.txt
root@hojikov:/var/www/html/blog# nginx -s reload
root@hojikov:/var/www/html/blog#
```

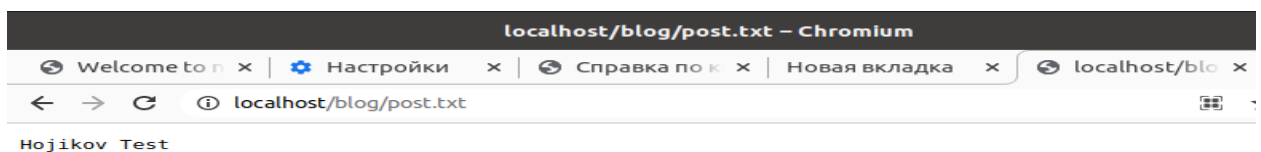
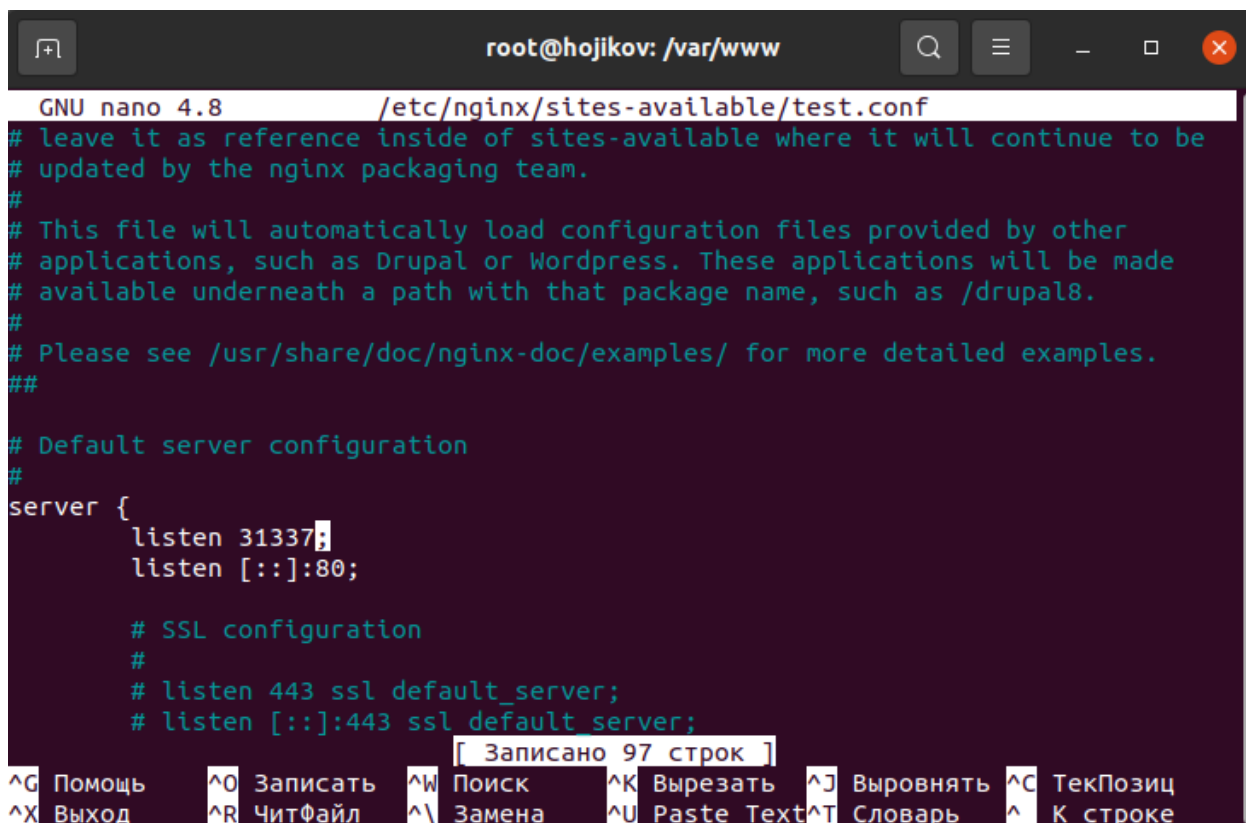


Рис. 7-8 создание текстового файла(post.txt) и запуск в URL со схемой http:

4. (*) Поменяйте порт, который слушает ваш сервер с 80 на 31337. Перезапустите сервер. Выполните задание 3 с учетом того, что сервер слушает на новом порту.

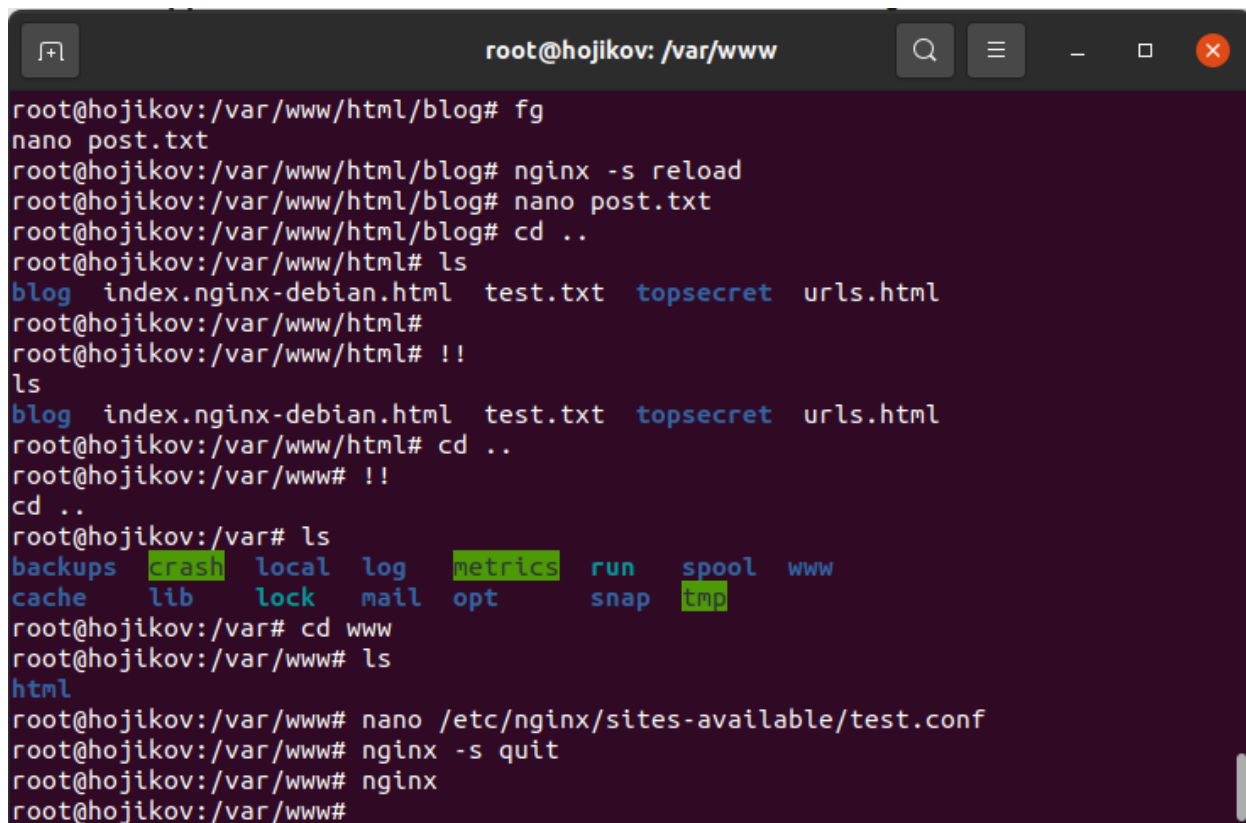


```
root@hojikov: /var/www
GNU nano 4.8 /etc/nginx/sites-available/test.conf
# leave it as reference inside of sites-available where it will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files provided by other
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
    listen 31337;
    listen [::]:80;

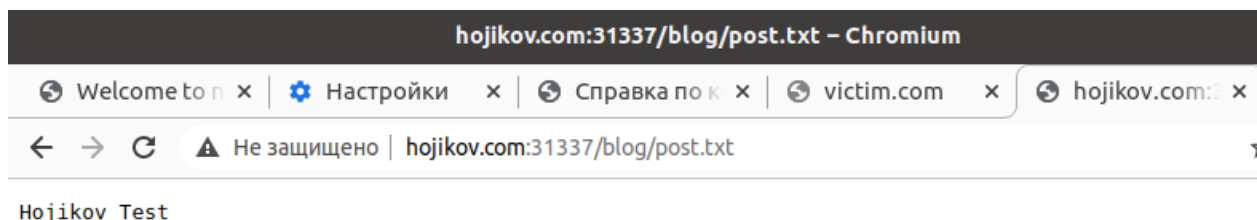
    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    [ Записано 97 строк ]
^G Помощь ^O Записать ^W Поиск ^K Вырезать ^J Выводить ^C ТекПозиц
^X Выход ^R ЧитФайл ^\ Замена ^U Paste Text ^T Словарь ^_ К строке
```

Рис.9 смена порта nginx с 80 на 31337 в конфигурационном файле test.conf



```
root@hojikov: /var/www
root@hojikov:/var/www/html/blog# fg
nano post.txt
root@hojikov:/var/www/html/blog# nginx -s reload
root@hojikov:/var/www/html/blog# nano post.txt
root@hojikov:/var/www/html/blog# cd ..
root@hojikov:/var/www/html# ls
blog index.nginx-debian.html test.txt topsecret urls.html
root@hojikov:/var/www/html#
root@hojikov:/var/www/html# !!
ls
blog index.nginx-debian.html test.txt topsecret urls.html
root@hojikov:/var/www/html# cd ..
root@hojikov:/var/www# !!
cd ..
root@hojikov:/var# ls
backups crash local log metrics run spool www
cache lib lock mail opt snap tmp
root@hojikov:/var# cd www
root@hojikov:/var/www# ls
html
root@hojikov:/var/www# nano /etc/nginx/sites-available/test.conf
root@hojikov:/var/www# nginx -s quit
root@hojikov:/var/www# nginx
root@hojikov:/var/www#
```

Рис 10 .Перезагрузка сервера после смены портов



```
root@hojikov: ~  
Следующие НОВЫЕ пакеты будут установлены:  
  net-tools  
Обновлено 0 пакетов, установлено 1 новых пакетов, для удаления отмечено 0 пакетов,  
и 4 пакетов не обновлено.  
Необходимо скачать 196 kB архивов.  
После данной операции объем занятого дискового пространства возрастёт на 864 kB.  
Пол:1 http://ru.archive.ubuntu.com/ubuntu focal/main amd64 net-tools amd64 1.60+  
git20180626.aebd88e-1ubuntu1 [196 kB]  
Получено 196 kB за 0с (874 kB/s)  
Выбор ранее не выбранного пакета net-tools.  
(Чтение базы данных ... на данный момент установлено 163949 файлов и каталогов.)  
Подготовка к распаковке .../net-tools_1.60+git20180626.aebd88e-1ubuntu1_amd64.deb  
...  
Распаковывается net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...  
Настраивается пакет net-tools (1.60+git20180626.aebd88e-1ubuntu1) ...  
Обрабатываются триггеры для man-db (2.9.1-1) ...  
root@hojikov:~# netstat -ntl  
Активные соединения с интернетом (only servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State  
tcp        0      0 127.0.0.53:53          0.0.0.0:*        LISTEN  
tcp        0      0 127.0.0.1:631          0.0.0.0:*        LISTEN  
tcp        0      0 0.0.0.0:31337          0.0.0.0:*        LISTEN  
tcp6       0      0 :::1:631               :::*             LISTEN  
root@hojikov:~#
```

Рис 11. Как видно на скрине и в браузере и в терминале порт 31337 работает и/или прослушивается!