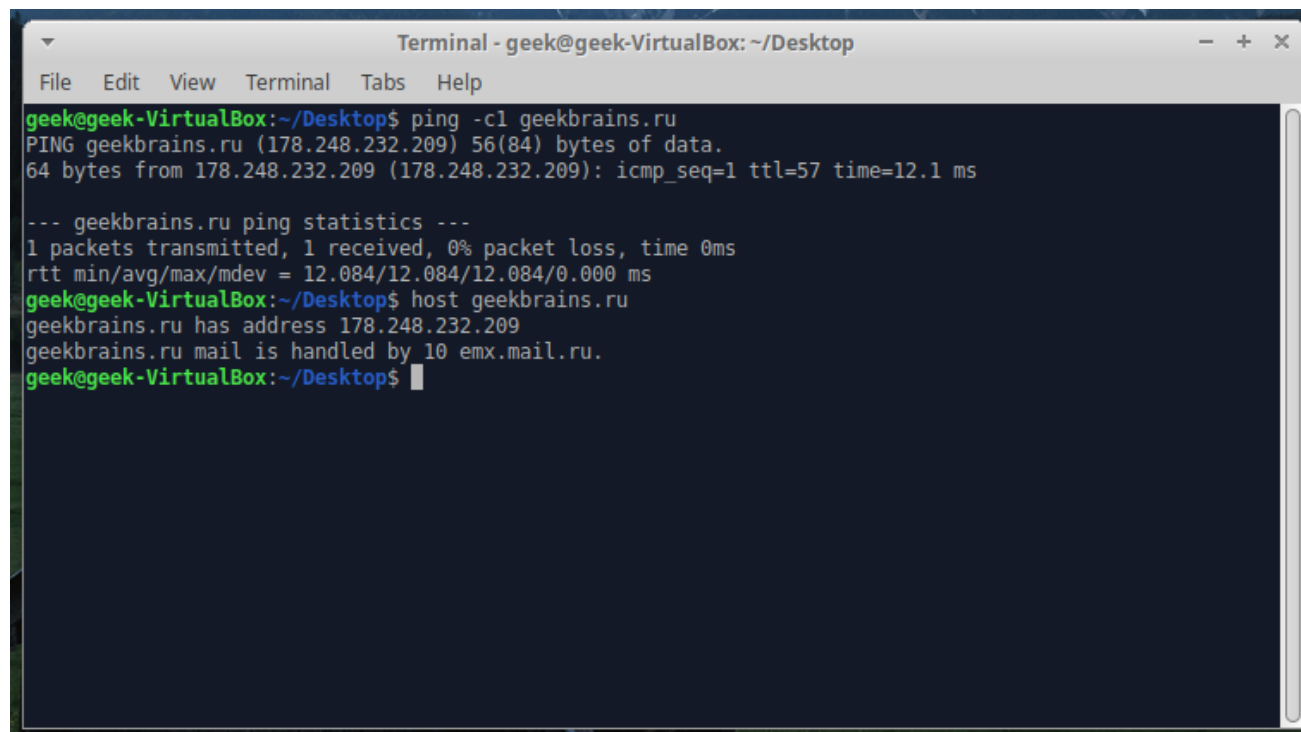


Коротков Сергей

Урок 2.

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

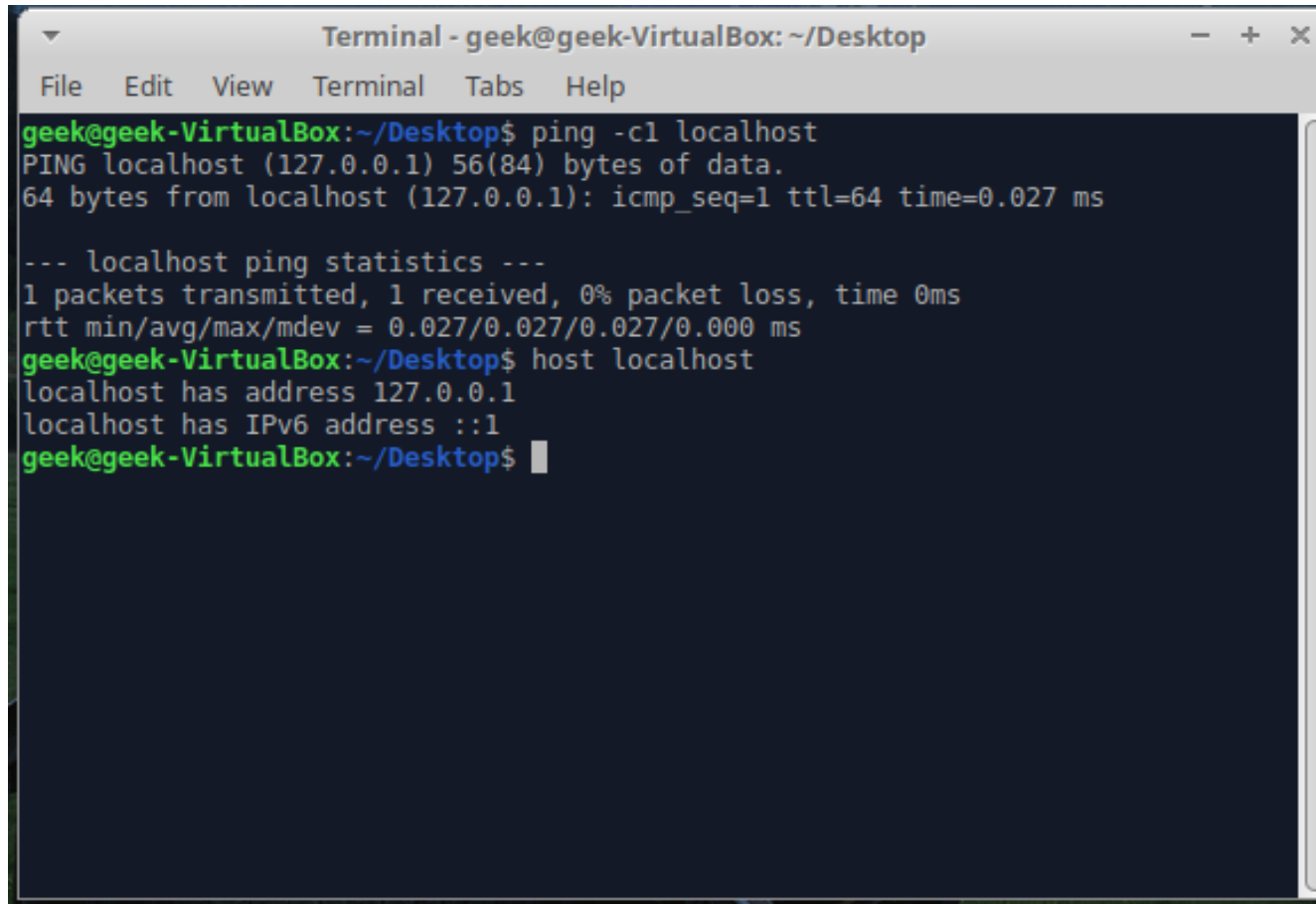
1.IP адрес сайта <https://geekbrains.ru>. 178.248.232.209



```
Terminal - geek@geek-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ ping -c1 geekbrains.ru
PING geekbrains.ru (178.248.232.209) 56(84) bytes of data.
64 bytes from 178.248.232.209 (178.248.232.209): icmp_seq=1 ttl=57 time=12.1 ms

--- geekbrains.ru ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.084/12.084/12.084/0.000 ms
geek@geek-VirtualBox:~/Desktop$ host geekbrains.ru
geekbrains.ru has address 178.248.232.209
geekbrains.ru mail is handled by 10 emx.mail.ru.
geek@geek-VirtualBox:~/Desktop$
```

2. IP адрес <http://localhost>. 127.0.0.1

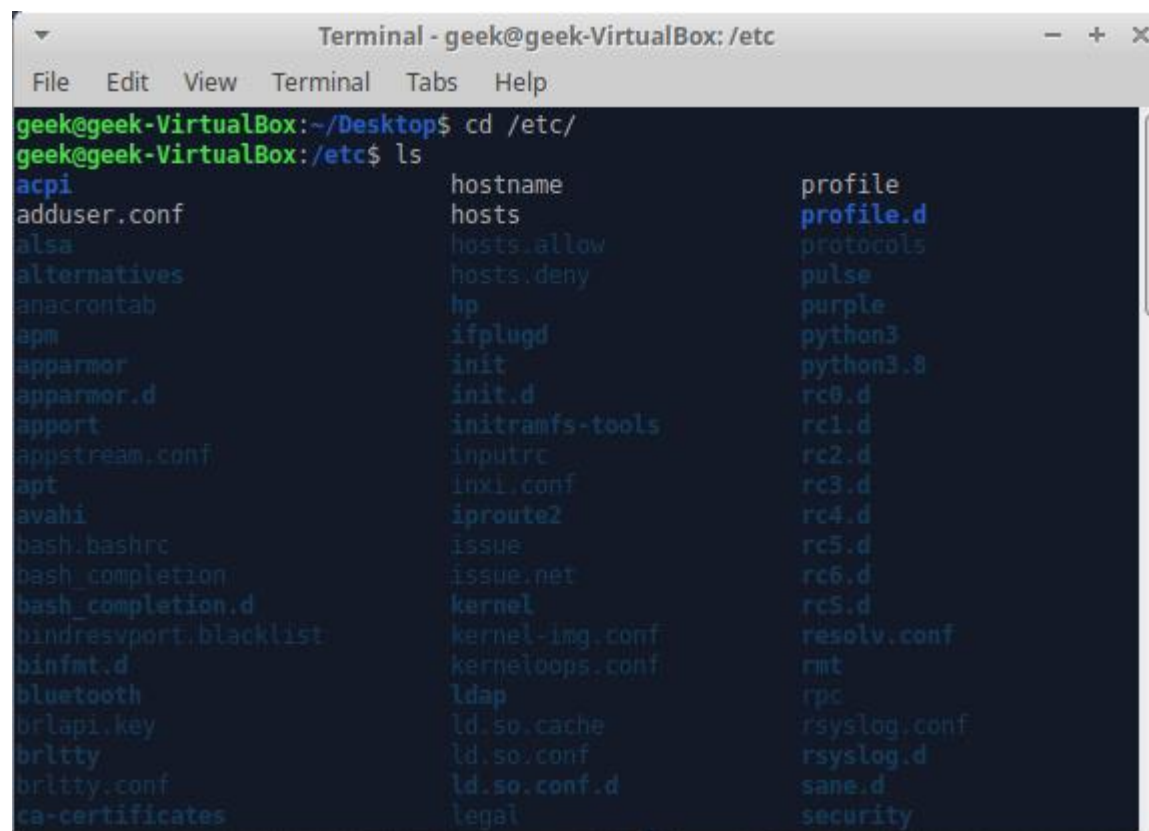
A terminal window titled "Terminal - geek@geek-VirtualBox: ~/Desktop" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the execution of two commands: a ping test and a host lookup. The ping test shows a successful connection to localhost (127.0.0.1) with a response time of 0.027 ms. The host lookup command shows the IP and IPv6 addresses for localhost.

```
Terminal - geek@geek-VirtualBox: ~/Desktop
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ ping -c1 localhost
PING localhost (127.0.0.1) 56(84) bytes of data:
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.027 ms

--- localhost ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.027/0.027/0.027/0.000 ms
geek@geek-VirtualBox:~/Desktop$ host localhost
localhost has address 127.0.0.1
localhost has IPv6 address ::1
geek@geek-VirtualBox:~/Desktop$
```

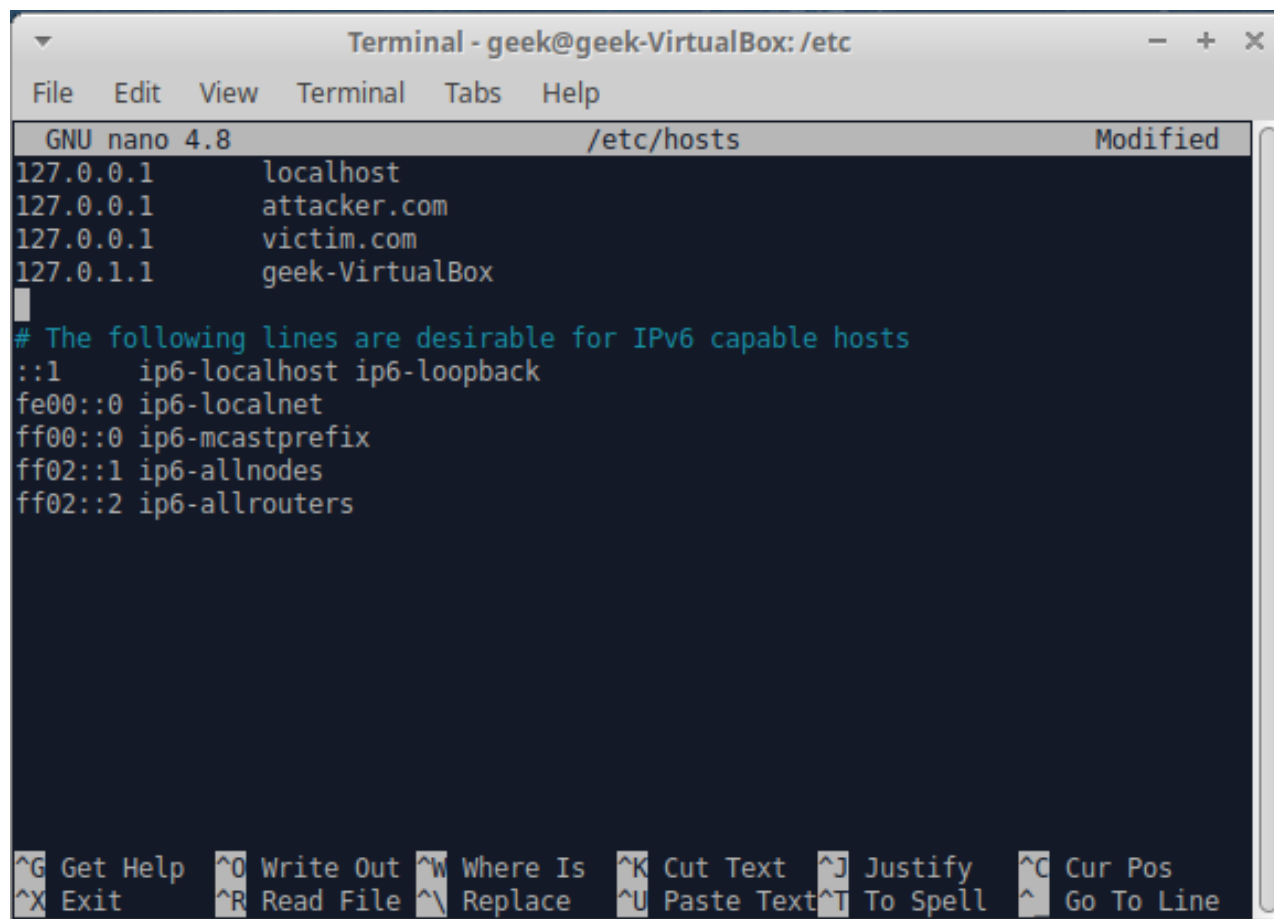
2. Найти файл hosts на своем компьютере (виртуальной машине). Сделать так, чтобы адрес сайта <http://attacker.com> и <http://victim.com> соответствовал адрес <http://localhost>.

1. Нашел файл hosts на своем компьютере (виртуальной машине).



```
Terminal - geek@geek-VirtualBox: /etc
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ cd /etc/
geek@geek-VirtualBox:/etc$ ls
acpi                               hostname                          profile
adduser.conf                      hosts                            profile.d
alsa                              hosts.allow                      protocols
alternatives                     hosts.deny                       pulse
anacrontab                       hp                               purple
apm                               ifplugd                         python3
apparmor                          init                            python3.8
apparmor.d                       init.d                          rc0.d
appport                           initramfs-tools                 rc1.d
appstream.conf                   inputrc                         rc2.d
apt                               inxi.conf                      rc3.d
avahi                            iproute2                       rc4.d
bash.bashrc                      issue                           rc5.d
bash_completion                  issue.net                       rc6.d
bash_completion.d                kernel                          rcS.d
bindresvport.blacklist           kernel-img.conf                resolv.conf
binfmt.d                         kerneloops.conf                rmt
bluetooth                       ldap                             rpc
brlapi.key                      ld.so.cache                    rsyslog.conf
brlitty                          ld.so.conf                     rsyslog.d
brlitty.conf                    ld.so.conf.d                   sane.d
ca-certificates                  legal                           security
```

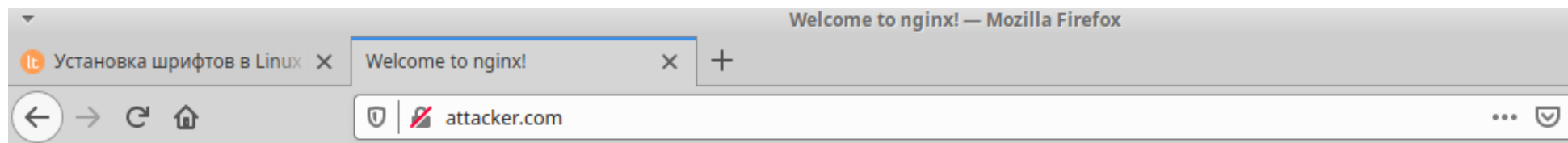
2. Чтобы домен attacker.com и victim.com ставился в соответствие адресу localhost, необходимо изменить файл hosts:



The image shows a terminal window titled "Terminal - geek@geek-VirtualBox: /etc". Inside, the GNU nano 4.8 editor is open, displaying the contents of the /etc/hosts file. The file lists four entries mapping IP addresses to hostnames: 127.0.0.1 to localhost, 127.0.0.1 to attacker.com, 127.0.0.1 to victim.com, and 127.0.1.1 to geek-VirtualBox. Below these, there is a comment and several IPv6-related entries. The bottom of the window shows a status bar with various nano editor shortcuts.

```
Terminal - geek@geek-VirtualBox: /etc
File Edit View Terminal Tabs Help
GNU nano 4.8 /etc/hosts Modified
127.0.0.1 localhost
127.0.0.1 attacker.com
127.0.0.1 victim.com
127.0.1.1 geek-VirtualBox
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

3. Теперь попробуем открыть в браузере `attacker.com` и `victim.com`. Открылся не `attacker.com` и `victim.com`, а наш сайт, где написано `Welcome to nginx`

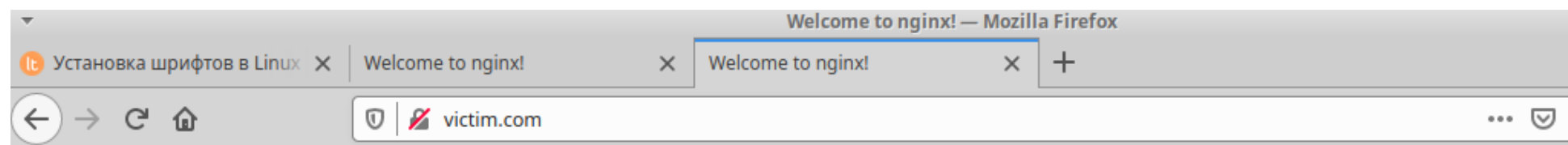


Welcome to nginx!

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.



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.

4. Изменился IP адрес <http://attacker.com> и <http://victim.com> на 127.0.0.1

```
geek@geek-VirtualBox:~/blog$ host attacker.com
attacker.com has address 127.0.0.1
geek@geek-VirtualBox:~/blog$ host victim.com
victim.com has address 127.0.0.1
victim.com mail is handled by 0 libel.victim.com.
victim.com mail is handled by 0 smallpox.victim.com.
geek@geek-VirtualBox:~/blog$
```

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.

1. Создал в корневом каталоге директорию **blog**:

```
geek@geek-VirtualBox:/etc$ cd
geek@geek-VirtualBox:~$ ls
BurpSuiteCommunity  Documents  'My Setting KSG.json'  Templates
cert.der            Downloads  Pictures               Videos
Desktop            Music     Public
geek@geek-VirtualBox:~$ mkdir blog
geek@geek-VirtualBox:~$ ls
blog          Desktop  Music  Public
BurpSuiteCommunity  Documents  'My Setting KSG.json'  Templates
cert.der           Downloads  Pictures               Videos
geek@geek-VirtualBox:~$
```

2. В директории создал файл **post.txt** . :

```
geek@geek-VirtualBox:~$ cd blog/  
geek@geek-VirtualBox:~/blog$ touch post.txt  
geek@geek-VirtualBox:~/blog$ ls  
post.txt  
geek@geek-VirtualBox:~/blog$
```

3. Составил полный URL со схемой *http* к этому файлу: **file:///home/geek/blog/post.txt**.

4. Запросил его через браузер:



A screenshot of a web browser window. The address bar shows the file path `file:///home/geek/blog/post.txt`. The browser interface includes back, forward, and refresh buttons.

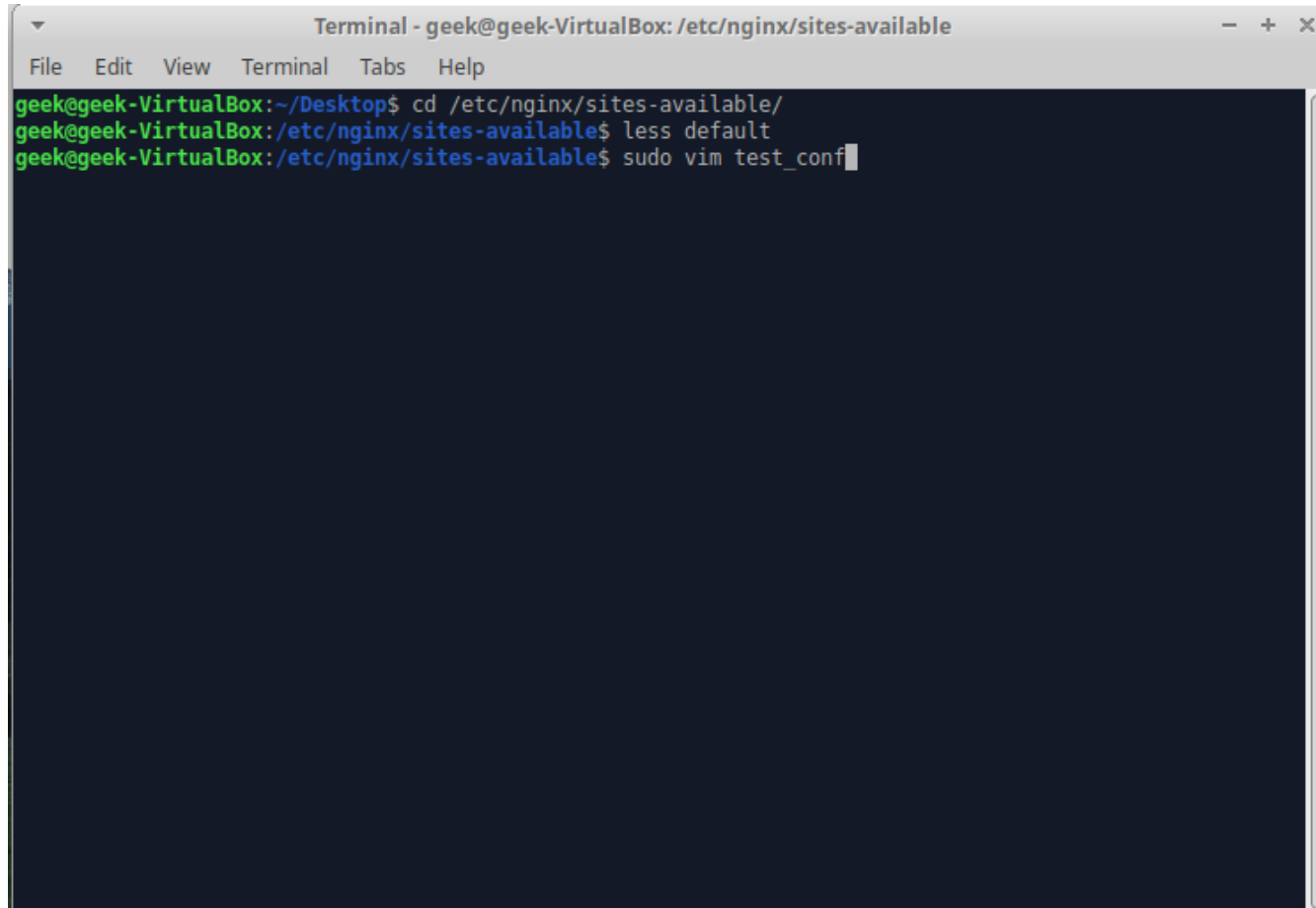
Hello, Sergey !!!!

Я помню чудное мгновенье:
Передо мной явилась ты,
Как мимолетное виденье,
Как гений чистой красоты.

Александр Пушкин.

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.

1. *Внесем изменения в файл test.conf при помощи текстового редактора Vim:*



```
Terminal - geek@geek-VirtualBox: /etc/nginx/sites-available
File Edit View Terminal Tabs Help
geek@geek-VirtualBox:~/Desktop$ cd /etc/nginx/sites-available/
geek@geek-VirtualBox:/etc/nginx/sites-available$ less default
geek@geek-VirtualBox:/etc/nginx/sites-available$ sudo vim test_conf
```


2. Поменял пор с 80 на 31337:

```
Terminal - geek@geek-VirtualBox: /etc/nginx/sites-enabled
File Edit View Terminal Tabs Help

##
# You should look at the following URL's in order to grasp a solid understanding
# of Nginx configuration files in order to fully unleash the power of Nginx.
# https://www.nginx.com/resources/wiki/start/
# https://www.nginx.com/resources/wiki/start/topics/tutorials/config_pitfalls/
# https://wiki.debian.org/Nginx/DirectoryStructure
#
# In most cases, administrators will remove this file from sites-enabled/ and
# 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;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure configuration.
    # See: https://bugs.debian.org/765782
    #
    # Self signed certs generated by the ssl-cert package
    # Don't use them in a production server!
    #
    # include snippets/snakeoil.conf;

    root /var/www/html;

    # Add index.php to the list if you are using PHP
    index index.html index.htm index.nginx-debian.html;

    server_name localhost;

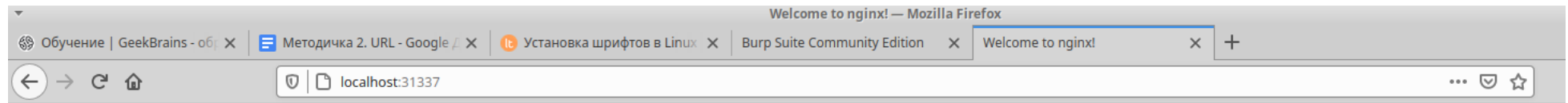
    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
    }

    # pass PHP scripts to FastCGI server
    #
    location ~ \.php$ {
-- INSERT --
```

24,1

Top

3. Проверяем в браузере: **localhost:31337** . Все работает.



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.

4.Выполнил задание 3 с учетом того, что сервер слушает на новом порту. Запрос на сервер не посылается, браузер на прямую открывает файл с нашего ПК.



Hello, Sergey !!!!

Я помню чудное мгновенье:
Передо мной явилась ты,
Как мимолетное виденье,
Как гений чистой красоты.

Александр Пушкин.