

## Урок 2. URL

### Оглавление

1. Открыть терминал. Установить программы host и whois (если уже не установлены). Выяснить IP адрес сайта <https://geekbrains.ru>. Выяснить IP адрес <http://localhost>. .....2
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>. .....4
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. ....5
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. ....5

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

1.1. Установим утилиты host и whois, выполним команды

```
sudo apt install host
```

```
sudo apt install whois
```

1.2. Узнаем ip адрес, выполним команду `host geekbrains.ru`

```
geekbrains.ru has address 178.248.232.209
```

```
geekbrains.ru mail is handled by 10 emx.mail.ru.
```

1.3. Узнаем информацию о владельце ip адреса, выполним команду `whois 178.248.232.209`

```
% This is the RIPE Database query service.
```

```
% The objects are in RPSL format.
```

```
%
```

```
% The RIPE Database is subject to Terms and Conditions.
```

```
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
```

```
% Note: this output has been filtered.
```

```
% To receive output for a database update, use the "-B" flag.
```

```
% Information related to '178.248.232.209 - 178.248.232.209'
```

```
% Abuse contact for '178.248.232.209 - 178.248.232.209' is 'abuse@qrator.net'
```

```
inetnum: 178.248.232.209 - 178.248.232.209
```

```
netname: QRATOR-10602
```

```
descr: ООО "GikBreins"
```

```
descr: 125167, g.Moskva, Leningradskij pr-kt, d.39, str.79
```

```
country: RU
```

```
admin-c: QL-RIPE
```

```
tech-c: QL-RIPE
```

```
status: ASSIGNED PA
```

```
mnt-by: MNT-QRATOR
```

```
mnt-by: MNT-QROBOT
```

```
created: 2020-11-27T16:07:51Z
```

```
last-modified: 2020-11-27T16:07:51Z
```

source: RIPE

role: Qrator Labs

address: 1-y Magistralnyy tupik 5A, Suite D/304

address: Moscow 123290

address: Russian Federation

org: ORG-LA267-RIPE

admin-c: LA27-RIPE

tech-c: DS22641-RIPE

tech-c: AZ2391-RIPE

nic-hdl: QL-RIPE

mnt-by: MNT-QRATOR-LIR

created: 2015-11-07T19:21:50Z

last-modified: 2019-03-07T13:48:32Z

source: RIPE # Filtered

% Information related to '178.248.232.0/24AS197068'

route: 178.248.232.0/24

descr: "HLL" LLC

origin: AS197068

mnt-by: MNT-QRATOR

created: 2010-09-07T20:08:15Z

last-modified: 2020-08-18T14:54:02Z

source: RIPE # Filtered

% Information related to '178.248.232.0/24AS200449'

route: 178.248.232.0/24

descr: "HLL" LLC

origin: AS200449

mnt-by: MNT-QRATOR

created: 2021-04-20T22:35:53Z

last-modified: 2021-04-20T22:35:53Z

source: RIPE

% This query was served by the RIPE Database Query Service version 1.101 (BLAARKOP)

#### 1.4. Узнаем ip адрес localhost, выполним команду host localhost

localhost has address 127.0.0.1

localhost has IPv6 address ::1

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`.

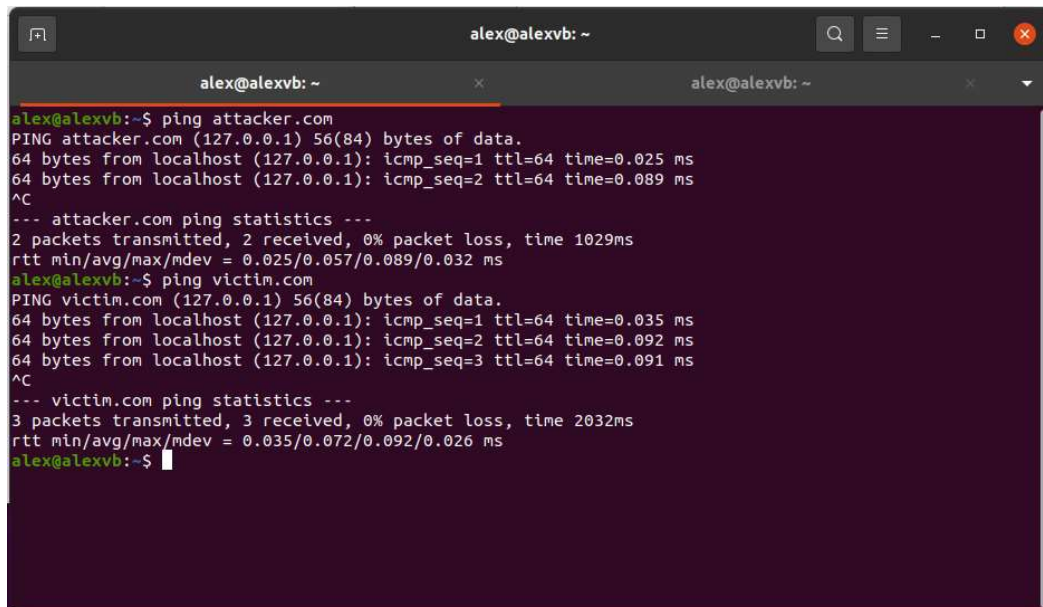
2.1. Команду `sudo vim /etc/hosts`

добавим строки

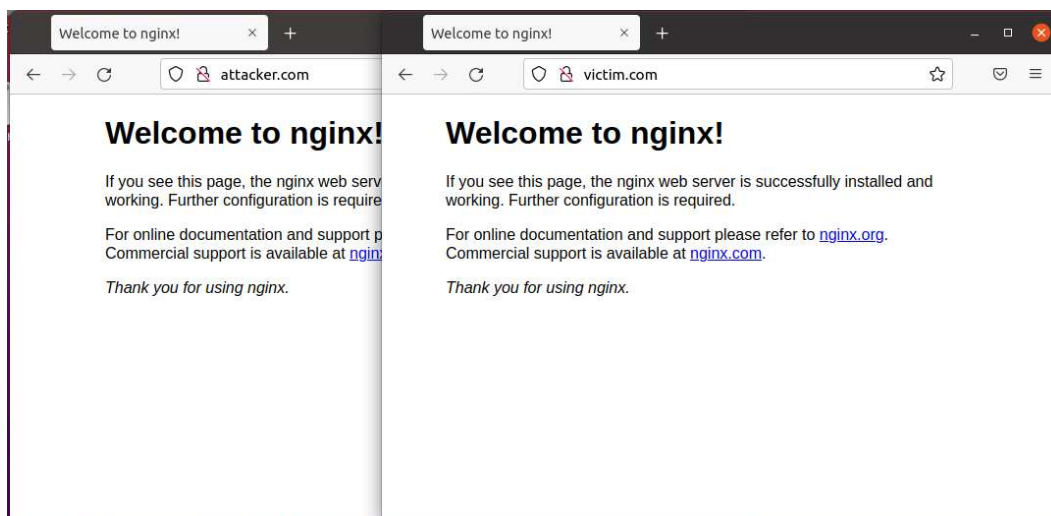
127.0.0.1 attacker.com

127.0.1.1 victim.com

2.2. Выполняем проверку



```
alex@alexvb: ~  
alex@alexvb:~$ ping attacker.com  
PING attacker.com (127.0.0.1) 56(84) bytes of data.  
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.025 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.089 ms  
^C  
--- attacker.com ping statistics ---  
2 packets transmitted, 2 received, 0% packet loss, time 1029ms  
rtt min/avg/max/ndev = 0.025/0.057/0.089/0.032 ms  
alex@alexvb:~$ ping victim.com  
PING victim.com (127.0.0.1) 56(84) bytes of data.  
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.035 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.092 ms  
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.091 ms  
^C  
--- victim.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2032ms  
rtt min/avg/max/ndev = 0.035/0.072/0.092/0.026 ms  
alex@alexvb:~$
```



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.

3.1. Создадим директорию blog, выполним команды

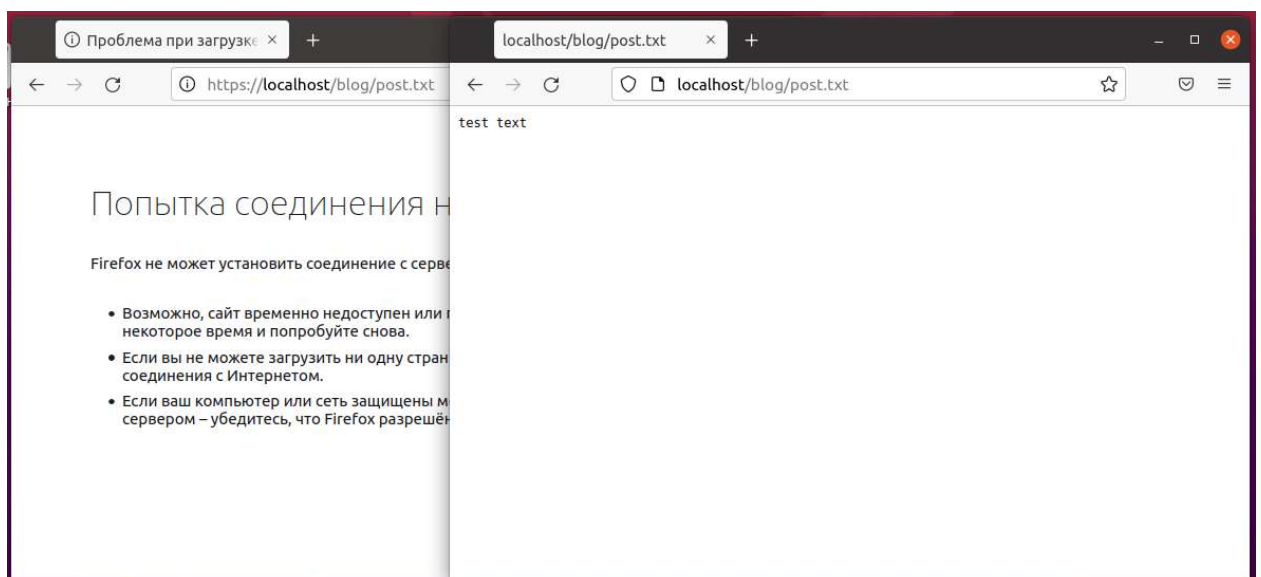
```
cd /usr/share/nginx/html/  
sudo mkdir blog
```

3.2. Создадим файл post.txt, выполним команды

```
cd blog  
sudo nano post.txt  
введем тестовую строку «test text»
```

3.3. Выполним проверку, в строке браузера введем <http://localhost/blog/post.txt>

<https://localhost/blog/post.txt>



По ssl сертификата нет, поэтому получаем ошибку

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.

4.1. Выполним настройку nginx, выполним команды

```
cd /etc/nginx/conf.d  
sudo nano basic.conf
```

```
alex@alexvb: /etc/nginx/conf.d
GNU nano 4.8 basic.conf
server {
    # listen      80;
    # listen      443;
    listen        31337;
    server_name    localhost;

    #access_log    /var/log/nginx/host.access.log  main;

    location / {
        root       /usr/share/nginx/html;
        index       index.html index.htm;
    }

    #error_page    404              /404.html;

    # redirect server error pages to the static page /50x.html
    #
    error_page     500 502 503 504  /50x.html;
    location = /50x.html {
        root        /usr/share/nginx/html;
    }
}
```

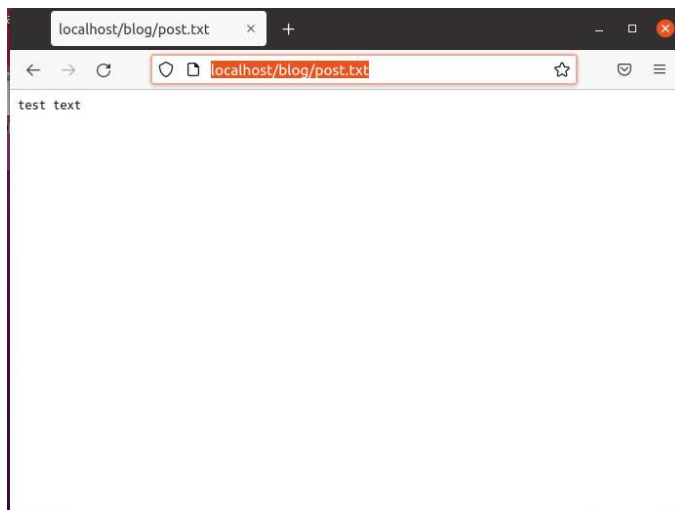
4.2. Применим новую конфигурацию nginx, выполним команду

`sudo systemctl stop nginx`

`sudo systemctl stop nginx`

4.3. В строке браузера введем

4.3.1. <http://localhost/blog/post.txt>, на 80 порту nginx по-прежнему работает



4.3.2. `https://localhost/blog/post.txt` , загружается, но блокируется браузером при загрузке, тк нет ssl сертификата

4.3.3. <http://localhost:31337/blog/post.txt>, теперь nginx слушает 31337 порт

