

Задания необходимо сдавать в формате скриншотов, которые сопровождаются комментариями. Отчет должен быть в pdf формате.

Пожалуйста, пишите в названии pdf файла домашнего задания своё имя.

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

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.

```
(kali㉿kali)-[~]
$ host geekbrains.ru
geekbrains.ru has address 178.248.232.209
geekbrains.ru mail is handled by 10 emx.mail.ru.

(kali㉿kali)-[~]
$ host localhost
localhost has address 127.0.0.1
localhost has IPv6 address ::1
```

```
(kali㉿kali)-[~]
$ 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:          000 "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
```

```
(kali@kali)~$ whois 127.0.0.1
```

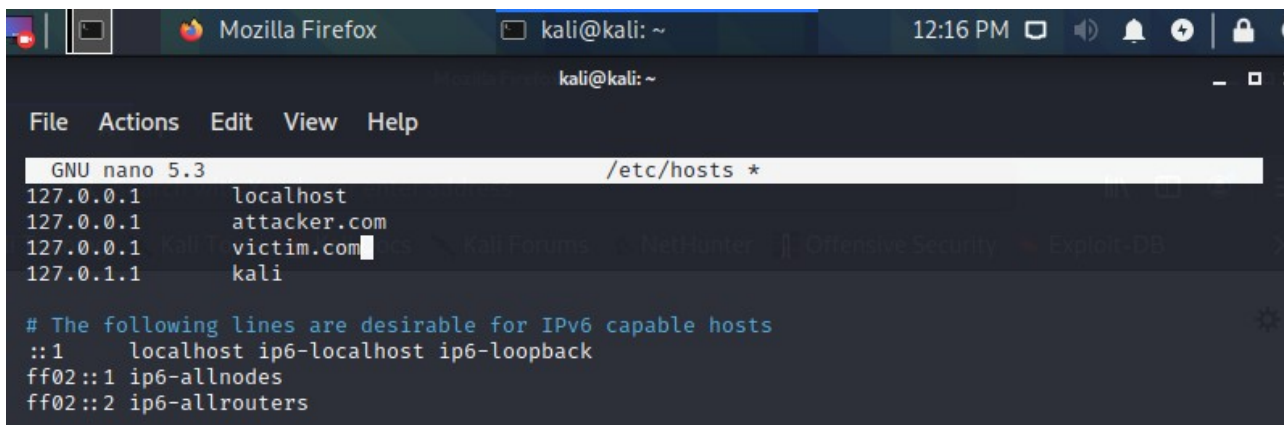
```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2021, American Registry for Internet Numbers, Ltd.
#

NetRange:      127.0.0.0 - 127.255.255.255
CIDR:          127.0.0.0/8
NetName:       SPECIAL-IPV4-LOOPBACK-IANA-RESERVED
NetHandle:     NET-127-0-0-0-1
Parent:        ()
NetType:       IANA Special Use
OriginAS:
Organization:  Internet Assigned Numbers Authority (IANA)
RegDate:
Updated:       2013-08-30
Comment:       Addresses starting with "127." are used when one program needs to talk to another program running on the same machine using the Internet
Comment:       Protocol. 127.0.0.1 is the most commonly used address and is called the "loopback" address.
Comment:
Comment:       These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Standard document, RFC 1122, which can be found here:
Comment:       http://datatracker.ietf.org/doc/rfc1122
Ref:           https://rdap.arin.net/registry/ip/127.0.0.0

OrgName:       Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:       2012-08-31
Ref:           https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgTechName:
OrgTechPhone:   +1-310-301-5820
OrgTechEmail:   abuse@iana.org
OrgTechRef:     https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```

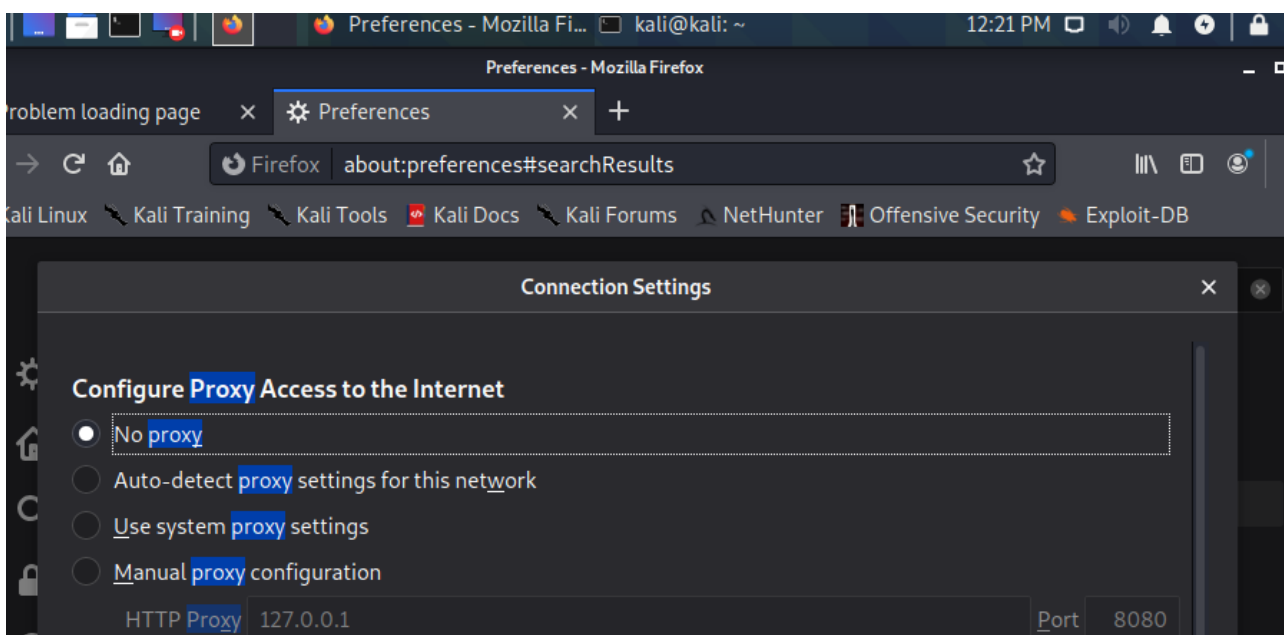
2. Меняем файл hosts



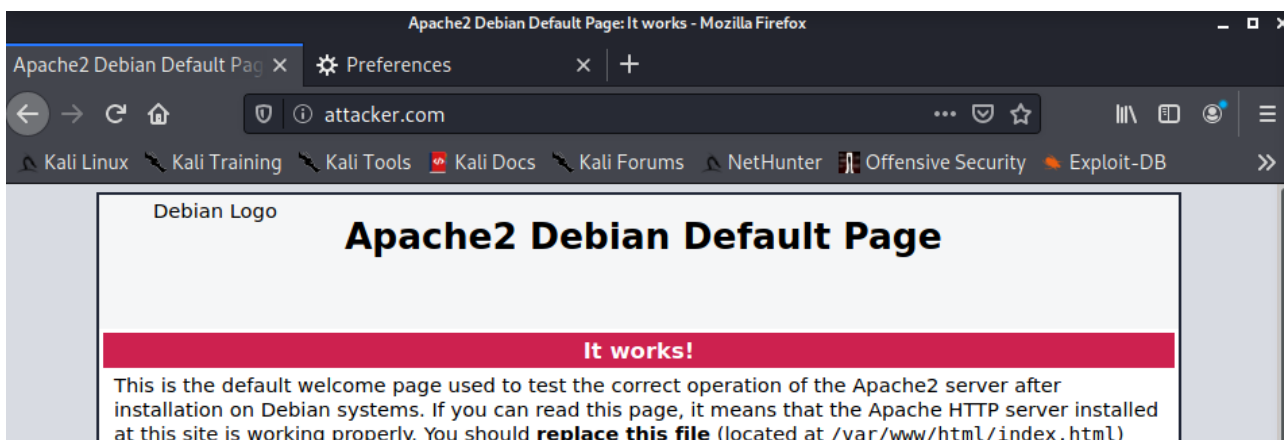
```
GNU nano 5.3 /etc/hosts *
127.0.0.1    localhost
127.0.0.1    attacker.com
127.0.0.1    victim.com
127.0.1.1    kali

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

Чтобы заработало также нужно выключить прокси в настройках Firefox.



Проверяем (у меня стоит стартовая страница apache2 в index.html)





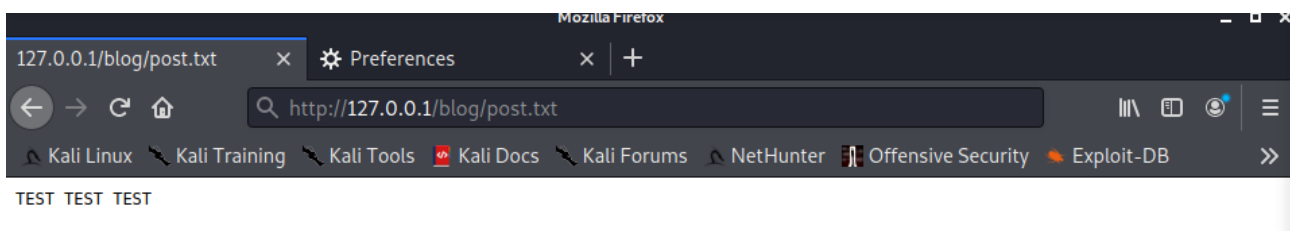
3. Создадим директорию и файл.

```
(kali@kali)-[/var/www/html]
$ ls
hello.html  hello.php  hello.txt  index.html  index.nginx-debian.html

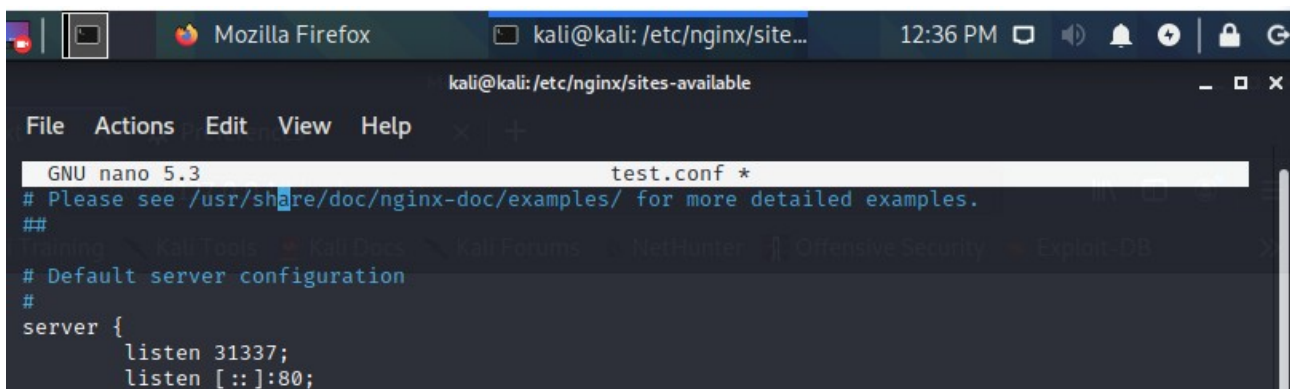
(kali@kali)-[/var/www/html]
$ sudo mkdir blog

(kali@kali)-[/var/www/html]
$ sudo nano blog/post.txt
```

Обратимся к нему через схему http(чтобы заработала https надо сделать сертификат и добавить его в firefox)



4. Поменяем порт в конфиге nginx



Перезапустим nginx

```
(kali@kali)-[/etc/nginx/sites-available]
$ sudo nginx -s quit

(kali@kali)-[/etc/nginx/sites-available]
$ sudo nginx
```


Проверим.

