

Практика 4 (сдать до 12.03.2021)

Лабораторная. Работа с DNS

Утилита nslookup

- Выполните nslookup, чтобы получить IP-адрес веб-сервера в Азии. Приложите скрин
- Выполните nslookup, чтобы определить авторитетные DNS-серверы для какого-либо университета в Европе. Приложите скрин

DNS-трассировка с использованием Wireshark

Задание А

Предварительная подготовка:

1. Используйте ipconfig для очистки кэша DNS на вашем компьютере.
2. Откройте браузер и очистите его кэш (для Internet Explorer можете использовать сочетание клавиш CTRL+Shift+Del).
3. Запустите Wireshark и введите ip.addr == ваш_IP_адрес в строке фильтра, где значение ваш_IP_адрес вы можете получить, используя утилиту ipconfig. Данный фильтр позволит нам отбросить все пакеты, не относящиеся к вашему хосту. Запустите процесс захвата пакетов в Wireshark.
4. Зайдите на страницу www.ietf.org в браузере.
5. Остановите захват пакетов.

Вопросы:

- Найдите DNS-запрос и ответ на него. С использованием какого транспортного протокола они отправлены?
- Какой порт назначения у запроса DNS?
- На какой IP-адрес отправлен DNS-запрос? Используйте ipconfig для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
- Посмотрите на последующий TCP-пакет с флагом SYN, отправленный вашим компьютером. Соответствует ли IP-адрес назначения пакета с SYN одному из адресов, приведенных в ответном сообщении DNS?
- Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

Задание В

Предварительная подготовка:

1. Запустите захват пакетов с тем же фильтром ip.addr == ваш_IP_адрес
2. Выполните команду nslookup для сервера www.spbu.ru.
3. Остановите захват
4. Вы увидите несколько пар запрос-ответ DNS. Найдите последнюю пару, все вопросы будут относиться к ней

Вопросы:

- Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?
- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Задание C

Повторите все шаги по предварительной подготовке из Задания B, но теперь для команды:

```
nslookup -type=NS spbu.ru
```

Вопросы:

- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Имена каких DNS-серверов Массачусетского института в нем содержатся? А есть ли их адреса в этом ответе?

Задание D

Снова повторите все шаги по предварительной подготовке из Задания B, но теперь для команды:

```
nslookup www.spbu.ru ns2.pu.ru
```

Вопросы:

- На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию? Если нет, то какому хосту он принадлежит?
- Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
- Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Сервисы whois

Выберите какой-либо сервис whois и получите имена двух DNS-серверов.

- Используйте команду nslookup на локальном хосте чтобы послать запросы трем серверам DNS: вашему локальному серверу DNS и двум найденным DNS-серверам
- Запустите запросы так, чтобы в DNS-ответах содержались различные типы ресурсных записей: A, NS и MX
- Используя nslookup, найдите веб-сервер, имеющий несколько IP-адресов

Задача. Веб-сервер на сокетах

Вам необходимо разработать простой веб-сервер, который будет обрабатывать только один запрос и работать в однопоточном режиме. Язык программирования вы можете выбрать любой.

Требования:

- веб-сервер создает сокет соединения при контакте с клиентом (браузером)
- получает HTTP-запрос из этого соединения
- анализирует запрос, чтобы определить конкретный запрашиваемый файл
- находит запрошенный файл в своей локальной файловой системе
- создает ответное HTTP-сообщение, состоящее из запрошенного файла и предшествующих ему строк заголовков
- отправляет ответ через TCP-соединение обратно клиенту.
- если браузер запрашивает файл, которого нет на веб-сервере, то сервер должен вернуть сообщение об ошибке «404 Not Found»

Ваша задача – разработать и запустить свой локальный веб-сервер, а затем проверить его работу при помощи отправки запросов через браузер. Можно проверить работу сервера, обращаясь к нему из браузеров с других хостов.

Скорее всего порт 80 у вас уже занят, поэтому вам необходимо использовать другой порт для работы вашей программы.