3. Лабораторная работа Wireshark: DNS

Служба DNS транслирует имена хостов в IP-адреса, выполняя важную роль в инфраструктуре сети Интернет. В этой лабораторной работе мы более внимательно ознакомимся с клиентской частью DNS. Напомним, что роль клиента в DNS относительно проста — клиент отправляет *запрос* своему локальному серверу DNS и получает обратно *ответ*.
Перед выполнением лабораторной необходимо изучить следующие материалы по службе DNS: **локальные DNS-сервера**, **DNS-кэширование**, **ресурсные записи DNS** и **их поля**.

nslookup

В этой работе мы будем пользоваться утилитой `nslookup`, доступной как на платформах Linux/Unix, так и на Microsoft. Для ее запуска наберите `nslookup` в командной строке. Общий синтаксис команды выглядит следующем образом:

```
nslookup –параметр1 –параметр2 имя_хоста dns-сервер
```

Команда `nslookup` может быть выполнена с несколькими параметрами, а может и без них. DNS-сервера тоже необязательно — в этом случае запрос будет обрабатывать локальный сервер DNS, установленный по умолчанию.

В качестве базовой функции утилита `nslookup` позволяет хосту, на котором она запущена, запрашивать записи с заданного сервера DNS. Запрашиваемым может быть корневой DNS-сервер, DNS-сервер верхнего уровня, авторитетный DNS-сервер или промежуточный сервер DNS. При выполнении данного задания утилита отправляет запрос указанному DNS-серверу, получает от него ответ и отображает результат.

Приведем примеры трех использований команды `nslookup`:

- `nslookup имя_хоста` – получение IP-адреса указанного хоста с информацией о DNS-сервере (как правило, выдается локальный DNS-сервер), предоставившем данный IP.
- `nslookup -type=NS имя_хоста` - запрос ресурсной записи типа NS у локального сервера DNS, т.е. получение имен и ip-адресов авторитетных DNS-серверов.
- `nslookup имя_хоста dns-сервер` - отослать запрос не серверу по умолчанию, а конкретно DNS-серверу.

Выполните следующие задания по nslookup:

1. Выполните `nslookup`, чтобы получить IP-адрес веб-сервера *petrsu.ru*. Какой адрес вы получили?

2. Выполните `nslookup`, чтобы определить авторитетные DNS-сервера для *petrsu.ru*. Какие у них адреса?
3. Выполните `nslookup` таким образом, чтобы задействовать конкретный DNS-сервер (не сервер по умолчанию) для получения IP-адрес веб-сервера *petrsu.ru.* В качестве адреса DNS-сервера можно использовать результат из п.2.

ipconfig

Утилиты `ipconfig` (для Windows) и `ifconfig` (для Linux/Unix) являются одними из наиболее простых и, в то же время, полезных команд для работы с сетевыми настройками. Ее можно использовать для отображения вашей текущей информации стека протоколов TCP/IP, включая адрес вашего хоста, адреса DNS-серверов, тип сетевого адаптера и т.д. Например, чтобы отобразить всю сетевую информацию вашего хоста, наберите

```
ipconfig /all
```

в командной строке, как показано на снимке ниже

Утилита `ipconfig` также очень полезна при работе с информацией службы DNS. Хост кэширует недавно полученные им DNS-записи. Чтобы их просмотреть, наберите команду:

```
ipconfig /displaydns
```

Каждая запись содержит срок жизни (TTL) в секундах. Чтобы очистить кэш DNS, наберите:

```
ipconfig /flushdns
```

Данная команда стирает все записи в кэше и загружает туда записи, находящиеся в файле *hosts*. (Windows: *C:\Windows\System32\drivers\etc,* Linux: /etc/hosts).

Выполните следующие задания по `ipconfig`

4. Выполните приведенные выше вариации команды *ipconfig,* изучите их вывод.

DNS-трассировка с использованием Wireshark

Теперь, после знакомства с утилитами `nslookup` и `ipconfig`, мы готовы приступить к основной части лабораторной. Давайте сначала перехватим пакеты DNS, которые создаются при обычном посещении веб-сайтов.

- Используйте `ipconfig` для очистки кэша DNS на вашем компьютере.
- Откройте браузер и очистите его кэш (можете использовать сочетание клавиш CTRL+Shift+Del).

- 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.
- Зайдите на страницу **www.ietf.org** в браузере. Остановите захват пакетов.

Ответьте на вопросы ниже.

5. Найдите DNS-запрос и ответ на него. С использованием UDP или TCP они отправлены?
6. Какой порт назначения у запроса DNS? Каков исходящий порт у DNS-ответа?
7. На какой IP-адрес отправлен DNS-запрос? Используйте ipconfig для определения IP-адреса вашего локального DNS-сервера. Одинаковы ли эти два адреса?
8. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
9. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?
10. 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?
11. Веб-страница содержит изображения. Выполняет ли хост новые запросы DNS перед загрузкой этих изображений?

Теперь поэкспериментируем с утилитой `nslookup`.

- Запустите захват пакетов.
- Выполните команду `nslookup` для сервера **petrsu.ru**.
- Остановите захват.

Ответьте на следующие вопросы:

12. Сколько пар DNS запрос-ответ появилось в списке?
13. Рассмотрите пару с type A. Каков порт назначения в запросе DNS? Какой порт источника в DNS-ответе?
14. На какой IP-адрес отправлен DNS-запрос? Совпадает ли он с адресом локального DNS-сервера, установленного по умолчанию?
15. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
16. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?

Повторим эксперимент, но теперь выполним команду:

```
nslookup –type=NS petrsu.ru
```

Ответьте на следующие вопросы:

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

А теперь повторим, используя следующую команду:

```
nslookup petrsu.ru 193.232.254.218 (или 8.8.8.8)
```

Ответьте на следующие вопросы:

20. 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?
21. Проанализируйте сообщение-запрос DNS. Запись какого типа запрашивается? Содержатся ли в запросе какие-нибудь «ответы»?
22. Проанализируйте ответное сообщение DNS. Сколько в нем «ответов»? Что содержится в каждом?