Лабораторна робота - Відстеження DNS-перетворень

Цілі та задачі

Частина 1. Спостереження за перетвореннями протоколу DNS URL-адрес на IP-адреси

Частина 2. Дослідження DNS-пошуку адреси веб-сайту за допомогою команди nslookup

Частина 3. Дослідження DNS-пошуку поштових серверів за допомогою команди nslookup

Довідкова інформація / Сценарій

Система доменних імен (Domain Name System, DNS) викликається під час уведення в адресному рядку веб-браузера Уніфікованого покажчика ресурсів (Uniform Resource Locator, URL), наприклад **http://www.cisco.com**. Перша частина URL описує протокол, який використовується. Традиційно до них належать протокол передавання гіпертексту (HTTP), протокол передавання гіпертексту через рівень захищених сокетів (Secure Socket Layer, SSL) - (HTTPS) і протокол передавання файлів (FTP).

DNS використовує другу частину URL-адреси, у даному прикладі - www.cisco.com. DNS перетворює доменне ім'я (www.cisco.com) на IP-адресу, щоб вихідний вузол зміг досягти кінцевого сервера. У цій лабораторній роботі ви матимете можливість спостерігати за протоколом DNS у дії і скористаєтесь командою **nslookup** (пошук сервера імен) для отримання додаткової інформації про DNS.

Необхідні ресурси

1 PC (Windows із доступом до Інтернету і режиму командного рядка)

Частина 1: Спостереження за перетвореннями протоколу DNS URL-адрес на IP-адреси

a. Відкрийте вікно командного рядка Windows.

b. У командному рядку проінгуйте URL-адресу Інтернет-корпорації з призначення імен і номерів (ICANN) за адресою **www.icann.org**. ICANN координує DNS, IP-адреси, системи керування доменними іменами верхнього рівня та функції керування кореневими серверами. Комп'ютеру потрібно перетворити cisco.com на IP-адресу, щоб знати, куди надсилати пакети Інтернет-протоколу керуючих повідомлень (Internet Control Message Protocol, ICMP).

Перший рядок виводу відображає виконане за допомогою DNS перетворення **www.icann.org** на IP-адресу. Результат роботи DNS повинен бути доступний для перегляду, навіть якщо у вашому заклад використовується міжмережний екран, який запобігає пінгуванню, або якщо сервер призначення забороняє звертатися за допомогою команди ping до свого веб-сервера.

Примітка: Якщо ім'я домену перетворюється на адресу IPv6, використовуйте команду **ping -4 www.icann.org** для переходу на адресу IPv4, якщо потрібно.

Запишіть IP-адреси для www.icann.org.

c. Замість URL-адреси використайте для звернення у веб-браузері адреси IPv4 з кроку b. Введіть **https://192.0.32.7** у веб-браузері. Якщо вдалося отримати IPv6-адресу, її також можна застосувати: **https://[2620:0:2d0:200::7]**.

d. Зверніть увагу, що домашня веб-сторінка ICANN відображається без використання DNS.

Людям здебільшого легше запам'ятовувати слова, аніж цифри. Якщо ви скажете комусь перейти на **www.icann.org**, вони, ймовірно, пам'ятатимуть саме цю адресу, а не 192.0.32.7, яка, мабуть, важча для сприйняття. Комп'ютери оперують числами. DNS - це процес переклад слів у числа. Окрім цього, має місце ще одне перетворення інформації. Люди сприймають десяткові числа. Комп'ютери обробляють дані у двійковому форматі. Десяткова IP-адреса 192.0.32.7 у двійковому форматі має вигляд 11000000.00000000.00100000.00000111. Що станеться, якщо скопіювати ці двійкові значення і використати їх у браузері?

e. У режимі командного рядка пропінгуйте **www.cisco.com**.

Примітка: Якщо для доменного імені визначено адресу IPv6, скористайтесь командою **ping -4 www.cisco.com** для перетворення на IPv4, якщо потрібно.

```
C:\> ping www.cisco.com
```

```
C:\> ping -4 www.cisco.com
```

При використанні команди ping www.cisco.com чи отримали ви таку ж IP-адресу, що й у прикладі? Поясніть.

У адресному рядку браузера введіть IP-адресу, яку ви отримали при пінгуванні www.cisco.com. Чи відображається веб-сайт? Поясніть.

Частина 2: Дослідження DNS-пошуку адреси веб-сайту за допомогою команди nslookup

a. У командному рядку введіть команду **nslookup**. Ваш результат може відрізнятися від наведеного у прикладі.

```
C:\> nslookup
```

Який DNS-сервер використовується за замовчуванням?

b. Зверніть увагу на зміну позначки командного рядка на більше (>). Це ознака команди **nslookup**. З появою цієї позначки можна вводити команди, пов'язані з DNS.

У полі курсора введіть **?** для перегляду списку всіх команд, доступних для використання у режимі **nslookup** .

c. Введіть **www.cisco.com**.

```
> www.cisco.com
Default Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
Name: e2867.dsca.akamaiedge.net
Addresses: 2600:1404:a:395::b33
          2600:1404:a:38e:b33
          172.230.155.162
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgikey.net
          wwwds.cisco.com.edgakey.net.globalredir.akadns.net
```

Яка адреса IPv4 відповідає уведеному доменному імені?

Примітка: IP-адреса, що відповідає вашому розташуванню, найімовірніше, буде відрізнятися, оскільки Cisco використовує дзеркальні сервери у різних локаціях по всьому світу.

Чи збігається вона з IP-адресою, виявленою за допомогою команди **ping**?

Окрім IP-адреси 172.230.155.162, відображаються такі числа: 2600:1404:a:395::b33 і 2600:1404:a:38e::b33. Що вони позначають?

d. У режимі nslookup введіть IP-адресу веб-сервера Cisco, яку ви щойно виявили. За допомогою **nslookup** можна отримати доменне ім'я, якщо URL-адреса вам невідома.

```
> 172.230.155.162
Default Server: one.one.one.one
Address: 1.1.1.1

Name: a172-230-155-162.deploy.static.akamaitechnologies.com
Address: 172.230.155.162
```

Інструмент **nslookup** можна використовувати для перетворення доменних імен на IP-адреси. Також він дозволяє виконувати зворотні перетворення IP-адрес на доменні імена.

Використовуючи інструмент **nslookup**, запишіть IP-адреси, пов'язані з **www.google.com**.

Частина 3: Дослідження DNS-пошуку поштових серверів за допомогою команди nslookup

a. У режимі nslookup введіть **set type=mx**, щоб використати **nslookup** для визначення поштових серверів.

```
> set type=mx
```

b. У режимі nslookup введіть **cisco.com**.

```
> cisco.com
Server: one.one.one.one
Address: 1.1.1.1

Non-authoritative answer:
cisco.com MX preference = 20, mail exchanger = rcdn-mx-01.cisco.com
cisco.com MX preference = 30, mail exchanger = aer-mx-01.cisco.com
cisco.com MX preference = 10, mail exchanger = alln-mx-01.cisco.com
```

Резервування (налаштування більше одного поштового сервера) є одним з основоположних принципів побудови мережі. За його впровадження, у разі відмови одного з поштових серверів, комп'ютер намагається звернутися із запитом до іншого поштового сервера. Адміністратори електронної пошти використовують параметр **MX preference** аби визначити, до якого поштового сервера слід звертатися у першу чергу. Насамперед звертаються до поштового сервера з найнижчим показником **MX preference**. Беручи до уваги отримані вище дані, до якого поштового сервера спершу йтиме звернення при надсиланні листа до cisco.com?

c. У режимі nslookup введіть **exit**, щоб повернутися до звичайного режиму командного рядка ПК.

d. Введіть **ipconfig /all**.

Запишіть IP-адреси усіх DNS-серверів, які використовує ваш навчальний заклад.

Аналіз результатів дослідження

Яке основне призначення DNS?