IT304 Lab5
Analysis of DNS using wireshark

1 nslookup

In this lab, we'll make extensive use of the nslookup tool, which is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, you just type the nslookup command on the command line. To run it in Windows, open the Command Prompt and run nslookup on the command line. In it is most basic operation, nslookup tool allows the host running the tool to query any specified DNS server for a DNS record. The queried DNS server can be a root DNS server, a top-level-domain DNS server, an authoritative DNS server, or an intermediate DNS server. To accomplish this task, nslookup sends a DNS query to the specified DNS server, receives a DNS reply from that same DNS server, and displays the result.

The response from this command provides two pieces of information:

1. the name and IP address of the DNS server that provides the answer
2. the answer itself, which is the host name and IP address of the requested client.

However, nslookup also indicates that the answer is "non-authoritative," meaning that this answer came from the cache of some server rather than from an authoritative DNS server

Example: *nslookup www.google.come*

1.1 Get the name of authoritative servers

nslookup -type=ns google.com

This causes nslookup to send a query for a type-NS record to the default local DNS server. In words, the query is saying, "Please send me the host names of the authoritative DNS for google.com"

1.2 Send query to specific DNS server

nslookup google.com 8.8.8.8

this command sends DNS query to server 8.8.8.8 DNS server.

1.3 Exercise 1

1. Run nslookup to obtain the IP address of daiict.ac.in server.
2. Run nslookup to determine the authoritative DNS servers for daiict.ac.in server.
3. Run nslookup so that 8.8.4.4 is queried for the mail servers for google.com.

2 Ipconfig

ipconfig (for Windows) and ifconfig (for Linux/Unix) are among the most useful little utilities in your host, especially for debugging network issues. Here we'll only describe ipconfig, although the Linux/Unix ifconfig is very similar. ipconfig can be used to show your current TCP/IP information, including your address, DNS server addresses, adapter type and so on. For example,

1. if you want to see all this information about your host, simply enter:
   ipconfig
2. To see cached DNS record:
   ipconfig /displaydns
   Each entry shows the remaining Time to Live (TTL) in seconds.
3. To clear the cache, enter
   ipconfig /flushdns // Flushing the DNS cache clears all entries and reloads the entries from the hosts file.

3 Tracing DNS with wireshark

Before doing any experiment of this section run following command:
ipconfig/flushdns

3.1 Exercise 2: DNS query from browser

- Open your browser and empty your browser cache.
- Open Wireshark and enter "ip.addr == your IP address" into the filter, where you obtain your IP ddress (the IP address for the computer on which you are running Wireshark) with ipconfig. This filter removes all packets that neither originate nor are destined to your host.
- Start packet capture in Wireshark.
- With your browser, visit the Web page: `http://www.daiict.ac.in`
- Stop packet capture.

Answer following question

1. Locate the DNS query and response messages. Are they sent over UDP or TCP?
2. What is the destination port for the DNS query message? What is the source port of DNS response message?
3. To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?
4. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
5. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
6. Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
7. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

3.2 Exercise 3: DNS query using nslookup

- Start packet capture.
- Do an nslookup on www.daiict.ac.in
- Stop packet capture.

Answer following questions

1. What is the destination port for the DNS query message? What is the source port of DNS response message?
2. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
3. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
4. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
5. Provide a screenshot

3.3 Exercise 4: Finding name servers

- Start packet capture
- run *nslookup –type=NS daiict.ac.in*
- Stop packet capture

Answer following questions

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
2. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
3. Examine the DNS response message. What daiict name servers does the response message provide?
4. Provide a screenshot.

3.4 Exercise 5:DNS query to specific DNS server

- Start packet capture
- run *nslookup daiict.ac.in 8.8.8.8*
- Stop packet capture

Answer following questions

1. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?
2. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
3. Examine the DNS response message. How many "answers" are provided? What does each of these answers contain?
4. Provide a screenshot.

4 Submission guidelines

Submit a pdf which contains all answers and necessary screenshots