

## CIS 457: Data Communications

### Week 10 Assignment: Working with HTTP DNS

**Point Value:** 20 Pts, late submission policy (20%/day for up to 5 days)

**Due Date:** 3/22/2024 by 12:00 AM EST

#### Submission format:

The following reports will be submitted on Blackboard (BB) using each group member's account.

- (1) The entire assignment's solution in a PDF format (your contribution to the assignment)
- (2) Group's Agreed-upon solution in a PDF format.

**Note:** Missing an individual's contribution leads to receiving **NO** credit for the assignment.

### Lab Objectives

The purpose of this lab is to:

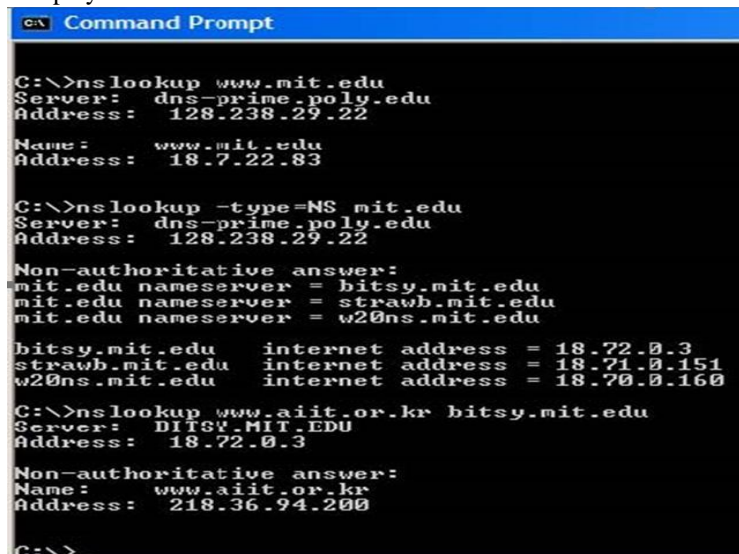
- Practice with the DNS's debugging/troubleshooting nslookup tool.
- Determine how DNS referral works.
- Identify possible DNS security threats and solutions.

### Introduction

The Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll look closer at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a query to its local DNS server and receives a response back. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated for the local DNS server, and a response is received from that server. Before beginning this lab, you may want to review DNS by reading Section 2.4 of the text. In particular, you may want to review the material on local DNS servers, DNS caching, DNS records and messages, and the TYPE field in the DNS record.

### Part 1. nslookup

In this lab, we'll extensively use the nslookup tool, which is available in most Linux/Unix and Microsoft platforms today. To run nslookup in Linux/Unix, type the nslookup command on the command line using the appropriate option. In its 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 (see the textbook for definitions of these terms). 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.



```

C:\>nslookup www.mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Name:    www.mit.edu
Address:  18.7.22.83

C:\>nslookup -type=NS mit.edu
Server:  dns-prime.poly.edu
Address:  128.238.29.22

Non-authoritative answer:
mit.edu nameserver = bitsy.mit.edu
mit.edu nameserver = strawb.mit.edu
mit.edu nameserver = w20ns.mit.edu

bitsy.mit.edu    internet address = 18.72.0.3
strawb.mit.edu   internet address = 18.71.0.151
w20ns.mit.edu    internet address = 18.70.0.160

C:\>nslookup www.aait.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address:  18.72.0.3

Non-authoritative answer:
Name:    www.aait.or.kr
Address:  218.36.94.200

C:\>
```

The above screenshot shows the results of three independent nslookup commands (displayed in the Windows Command Prompt). In this example, the client host is located on the campus of Polytechnic University in Brooklyn, where the default local DNS server is **dns-prime.poly.edu**. When running nslookup, if no DNS server is

specified, then nslookup sends the query to the default DNS server, which in this case is **dns-prime.poly.edu**. Consider the first command: nslookup www.mit.edu

In words, this command is saying “please send me the IP address for the host www.mit.edu”. As shown in the screenshot, **the response from this command provides two pieces of information:**

- (1) the name and IP address of the DNS server that provides the answer; and
- (2) the answer itself, which is the host name and IP address of [www.mit.edu](http://www.mit.edu).

Although the response came from the local DNS server at Polytechnic University, it is quite possible that this DNS server iteratively contacted several other DNS servers to get the answer, as described in the textbook.

- Now consider the second command: **nslookup -type=NS mit.edu**

In this example, we have provided the option “-type=NS” and the domain “mit.edu”. 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 mit.edu”. (When the -type option is not used, nslookup uses the default to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server providing the answer (the default local DNS server) along with three MIT nameservers. Each of these servers is an authoritative DNS server for the hosts on the MIT campus. 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 MIT DNS server.

Finally, the answer also includes the IP addresses of the authoritative DNS servers at MIT. (Even though the type-NS query generated by nslookup did not explicitly ask for the IP addresses, the local DNS server returned these “for free” and nslookup displays the result.)

- Now finally consider **the third command: nslookup [www.aiit.or.kr](http://www.aiit.or.kr) ns1-37.akam.net**

In this example, we indicate that we want the query to be sent to the DNS server **ns1-37.akam.net** of the mit.edu domain rather than the default DNS server (**dns-prime.poly.edu**). Thus, the query and reply transaction occurs directly between our querying host and **ns1-37.akam.net**. In this example, the DNS server **ns1-37.akam.net** is asked to provide the IP address of the host [www.aiit.or.kr](http://www.aiit.or.kr), which is a web server at the Advanced Institute of Information Technology (in Korea). Observe the result and analyze it. Now that we have reviewed a few illustrative examples, you may wonder about the general syntax of nslookup commands.

The syntax is: **nslookup -option1 -option2 [host-to-find](#) [dns-server-to-carry out-the-query](#)**

In general, nslookup can be run with zero, one, two, or more options. And as we have seen in the above examples, the dns-server is optional as well; if it is not supplied, the query is sent to the default local DNS server.

**Now that we have provided an overview of nslookup, it is time for you to test-drive it yourself. Do the following (and write down the results):**

**Q- 1. Run nslookup to obtain the IP address of any Web server in Asia. What is the IP address of that server?**

**Q- 2. Run nslookup to determine the DNS servers for a university in Europe. What is the DNS servers’ IP address?**

**Q- 3. Run nslookup so that one of the DNS servers obtained in Question 2 is queried for the mail servers for Yahoo! mail. Please, append . at the end of the domain name [mail.yahoo.com](mailto:mail.yahoo.com). to avoid having the dns appends a suffix for you. If the response is obtained, what is its IP address? If no response is obtained, do your research and explain why.**

## Part 2. Tracing DNS with Wireshark

Now that we know nslookup, we're ready to get down to some serious business. [Use](#) the trace file **dns-ethereal-trace-1** to answer the following questions. The trace was captured while we visited the Web page: <http://www.ietf.org>

- Q- 4. Locate the DNS query and response messages. Are they sent over UDP or TCP?
- Q- 5. What is the destination port for the DNS query message? What is the source port of DNS response message?
- Q- 6. To what IP address is the DNS query message sent?
- Q- 7. Examine the DNS query. What "Type" of DNS query is it? Does the query message contain any "answers"?
- Q- 8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
- Q- 9. Consider the subsequent TCP SYN packet sent by the client host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?
- Q- 10. This web page contains images. Before retrieving each image, does the client host issue new DNS queries?

[Use](#) the trace file **dns-ethereal-trace-2** to answer the following questions. The trace was captured while we used the nslookup against the Web page: [www.mit.edu](http://www.mit.edu).

- Q- 11. What is the destination port for the DNS query message related to the alias [www.mit.edu](http://www.mit.edu)? What is the source port of DNS response message?
- Q- 12. To what IP address is the DNS query message sent?
- Q- 13. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
- Q- 14. Examine the associated DNS response message. How many "answers" are provided? What do each of these answers contain?
- Q- 15. Provide a screenshot for the associated DNS response message.

[Use](#) the trace file **dns-ethereal-trace-3** to answer the following questions. The trace was captured while we used the nslookup against the domain [mit.edu](http://mit.edu) to obtain its type NS record.

- Q- 16. To what IP address is the DNS query message sent?
- Q- 17. Examine the DNS query message. What "Type" of DNS query is it?
- Q- 18. Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT nameservers? Provide a screenshot.
- Q- 19. What best TTL value would a server admin choose? when and why? (2 Points) You may use the following link as a reference for your research: [https://labs.ripe.net/author/giovane\\_moura/how-to-choose-dns-ttl-values/](https://labs.ripe.net/author/giovane_moura/how-to-choose-dns-ttl-values/)

Now, [use](#) the Wireshark trace file **dns-ethereal-trace-4** that has been captured using the command: **nslookup www.iiit.or.kr bitsy.mit.edu** to answer the following questions:

**Note** that if you try this command, you will get a different trace file because MIT recently turned off the DNS redirection feature on all of its NS servers.

- Q- 20. To what IP address is the DNS query message sent?
- Q- 21. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?
- Q-22. Examine the DNS response message. How many "answers" are provided? What does each answer contain?
- Q- 23. Describe how a hacker can launch a DNS spoofing attack against a corporate network. What mitigation solution should be used to protect against this attack? (2 Points)

**References:**

- Some of the materials are copied and compiled from the resources of Computer Networking: A Top-Down Approach (8<sup>th</sup> Edition) by James Kurose and Keith Ross.
- What best TTL value would you choose?  
[https://labs.ripe.net/author/giovane\\_moura/how-to-choose-dns-ttl-values/](https://labs.ripe.net/author/giovane_moura/how-to-choose-dns-ttl-values/)