

CIS 457- Lab06

Working with DNS Protocol

Due by: 10/16/2018

Total Points: **25 Points** (each question (Q1-Q22) worth 1Pt and Q23 worth 3Pts)

Submission format: hardcopy report per group of 2 students

Lab Objectives

The purpose of this lab is to:

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

Introduction

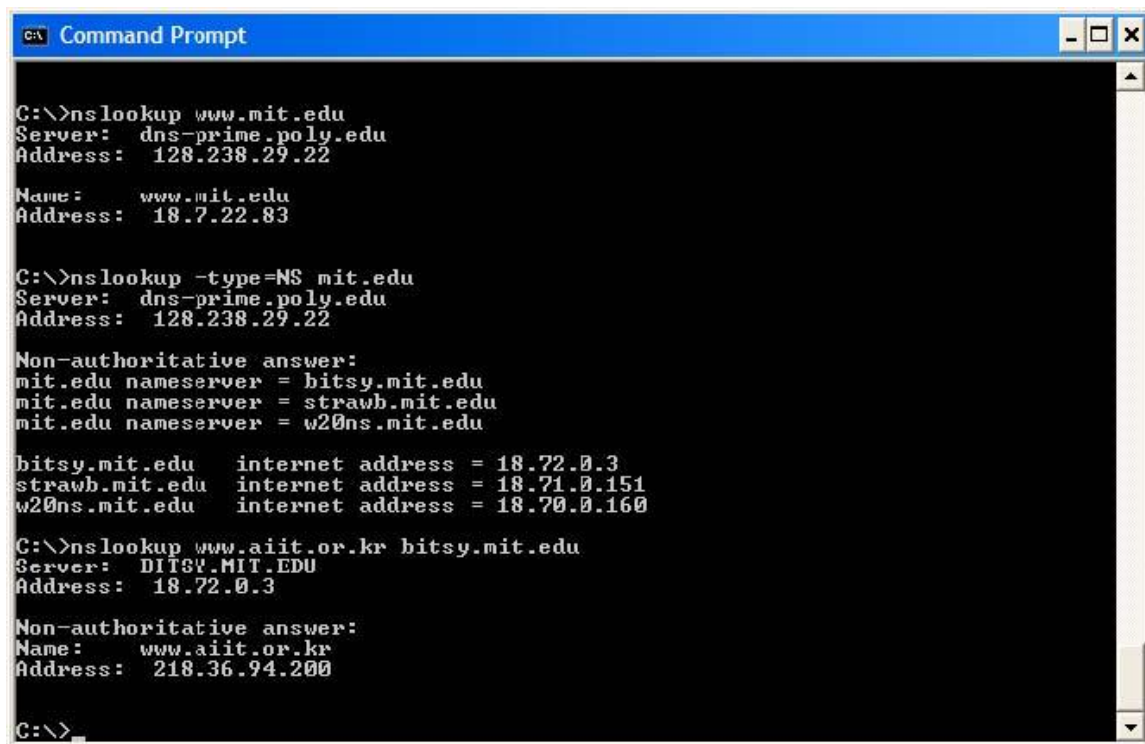
The Domain Name System (DNS) translates hostnames to IP addresses, fulfilling a critical role in the Internet infrastructure. In this lab, we'll take a closer look at the client side of DNS. Recall that the client's role in the DNS is relatively simple – a client sends a *query* to its local DNS server, and receives a *response* back. From the DNS client's standpoint, however, the protocol is quite simple – a query is formulated to 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 2.5 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 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.

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.aiit.or.kr bitsy.mit.edu
Server:  BITSY.MIT.EDU
Address: 18.72.0.3

Non-authoritative answer:
Name:    www.aiit.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 *dnsprime.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*. Although the response came from the local DNS server at Polytechnic University, it is quite possible that this local DNS server iteratively contacted several other DNS servers to get the answer, as described in Section 2.5 of 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, which is to query for type A records.) The answer, displayed in the above screenshot, first indicates the DNS server that is providing the answer (which is the default local DNS server) along with three MIT nameservers. Each of these servers is indeed 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 ns1-37.akam.net
```

In this example, we indicate that we want the query sent to the DNS server *ns1-37.akam.net* of the mit.edu domain rather than to the default DNS server (*dns-prime.poly.edu*). Thus, the query and reply transaction takes place 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*, which is a web server at the Advanced Institute of Information Technology (in Korea). Observe the result and analyze it.

Now that we have gone through a few illustrative examples, you are perhaps wondering about the general syntax of *nslookup* commands. The syntax is:

```
nslookup -option1 -option2 host-to-find dns-server
```

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):

1. Run *nslookup* to obtain the IP address of a Web server in Asia. What is the IP address of that server?
2. Run *nslookup* to determine the authoritative DNS servers for a university in Europe. What is the the authoritative DNS servers' IP address?
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* to avoid having the dns appends a suffix for you. If response is obtained, what is its IP address?

Part 2. Tracing DNS with Wireshark

Now that we are familiar with *nslookup*, we're ready to get down to some serious business. Let's first capture the DNS packets that are generated by ordinary Web-surfing activity.

- 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_address with ifconfig. 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.ietf.org>
- Stop packet capture.

Note: if you are unable to run Wireshark and capture a trace file, use the trace file **dns-ethereal-trace-1**. Answer the following questions. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use *File->Print*, choose *Selected packet only*, choose *Packet summary line*, and select the minimum amount of packet detail that you need to answer the question.

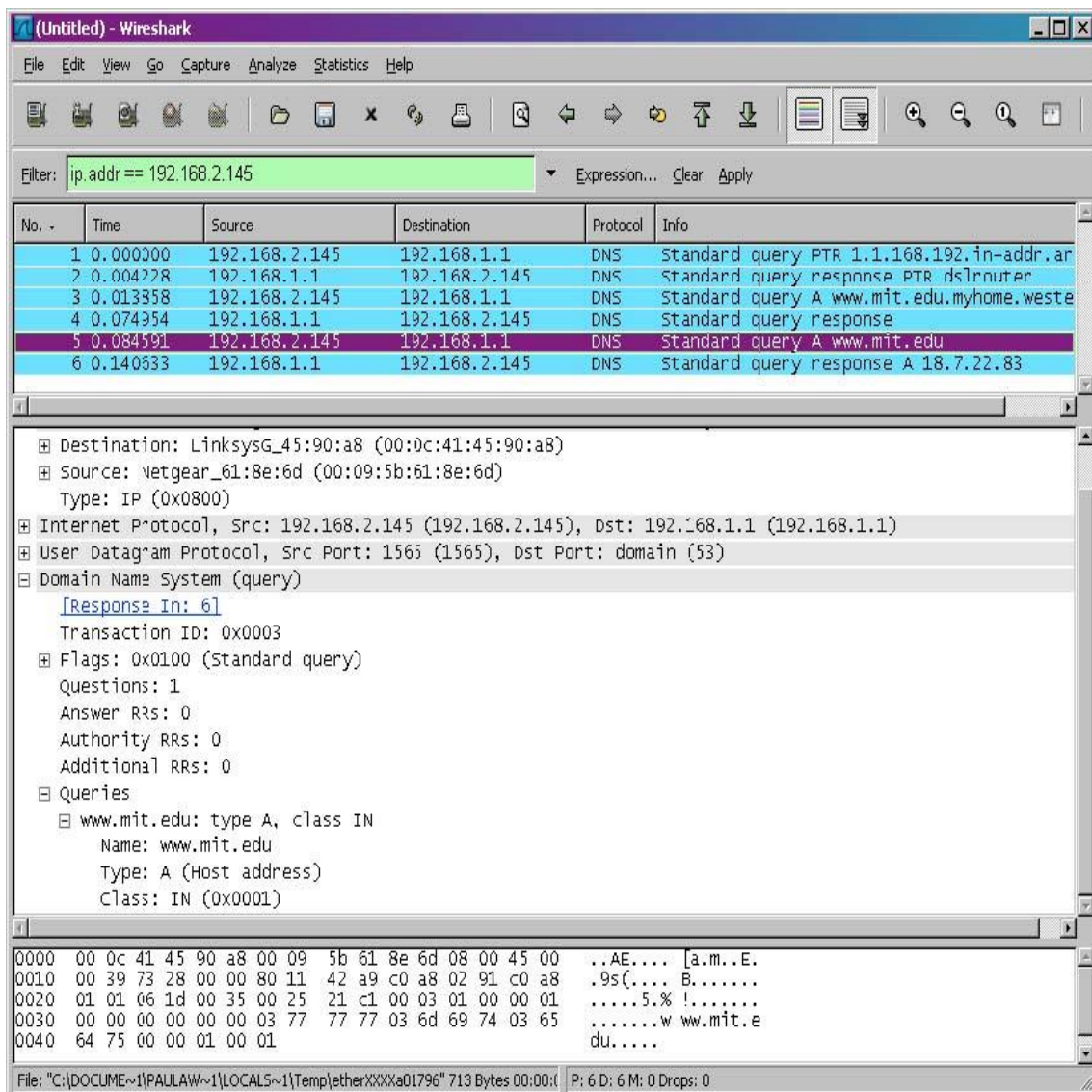
4. Locate the DNS query and response messages. Are then sent over UDP or TCP?
5. What is the destination port for the DNS query message? What is the source port of DNS response message?
6. To what IP address is the DNS query message sent? Use *nslookup* to determine the IP address of your local DNS server. Are these two IP addresses the same?
7. Examine the DNS query. What "Type" of DNS query is it? Does the query message contain any "answers"?
8. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?
9. 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?
10. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

Now let's use *nslookup*.

- Start packet capture.
- Do an *nslookup* on www.mit.edu
- Stop packet capture.

We see from the screenshot listed below that *nslookup* actually sent three DNS queries and received three DNS responses. For the purpose of this assignment, in answering the following questions, ignore the first two sets of queries/responses, as they are specific to *nslookup* and are not normally generated by standard Internet applications. You should instead focus on the last query and response messages.

Note: if you are unable to run Wireshark and capture a trace file, use the trace file [dns-ethereal-trace-2](#)



11. What is the destination port for the DNS query message? What is the source port of DNS response message?
12. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
13. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
14. Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?
15. Provide a screenshot.

Now repeat the previous experiment, but instead issue the command:

```
nslookup -type=NS mit.edu
```

If you are unable to run Wireshark and capture a trace file, use the trace file [dns-ethereal-trace-3](#)

Answer the following questions:

16. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?
17. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
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?
19. Provide a screenshot.

Now, use the Wireshark trace file [dns-ethereal-trace-4](#) that has been captured using the command: `nslookup www.aiit.or.kr bitsy.mit.edu`

Note that if you tried this command, you will get a different trace file because MIT has turned off the DNS redirection feature on its NS servers.

Answer the following questions:

20. To what IP address is the DNS query message sent?
21. Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?
22. Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?
23. Describe how a hacker can manage to launch DNS spoofing attack against corporate network. What mitigation solution should it be used to protect against this attack? (3 Points)

Reference:

- The lab materials are copied and compiled from the resources of the Computer Networking: A Top-Down Approach (7th Edition) 7th Edition book by James Kurose and Keith Ross.