Brian Hert
Badruddoja, Syed
CSC 138
14th, April 2024

Lab 3: Exploring DNS

1: Run nslookup to obtain the IP address of a Web server (www.amazon.com). What is the IP address of that server (There can be both IPv6 and IPv4 addresses)?

Server: ns4.csus.edu
Address: 169.237.38.37

Non-authoritative answer:
Name: www.amazon.com
Addresses: 205.251.242.103
205.251.244.103
205.251.246.103

2: Run nslookup to determine the authoritative DNS servers using the nslookup command with options -type=NS as shown earlier.

Server: ns4.csus.edu
Address: 169.237.38.37

Non-authoritative answer:
amazon.com nameserver = ns1.example.com
amazon.com nameserver = ns2.example.com

Authoritative answers can be found from:
ns1.amazon.com internet address = 192.0.2.1
ns2.amazon.com internet address = 192.0.2.2

3. Locate the DNS query and response messages. Are they sent over UDP or TCP?

They are sent over UDP

4. What is the destination port for the DNS query messages? What is the source port of DNS response messages?

The destination port for the DNS query messages is 53 and the source port for DNS response messages is 53.

5. To what IP address is the DNS query message sent? Use “ipconfig /all” to determine the IP address of your local DNS server. Are these two IP addresses the same?

The DNS query message sent was 192.168.1.1, which means that these two IP addresses aren't the same.

6. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

It's a type A Standard Query and it doesn't contain any answers.

7. Examine the DNS response message. How many "answers" are provided? What do each of these answers contain?

There are two answers containing information about the type of address, name of host, time-to-live, class, IP address and data length.

8. Consider the subsequent TCP SYN packet sent by your host post DNS response. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?

The first SYN packet was sent to 209.173.57.180 which corresponds to the first IP address provided in the DNS response message.

9. This web page contains images. Before retrieving each image, does your host issue new DNS queries?

No

10. What is the destination port for the DNS query message? What is the source port of DNS response messages?

The destination port of the DNS query is 53 and the source port of DNS response messages is 53.

11. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It's sent to 192.168.1.1 which is the IP address of the default local DNS server arranged on the client system.

12. Examine the DNS query message. What "Type" of DNS query is it? Does the query message contain any "answers"?

The DNS query is Type A and doesn't contain any answers.

13. Examine the DNS response message. How many "answers" are provided? What do each of

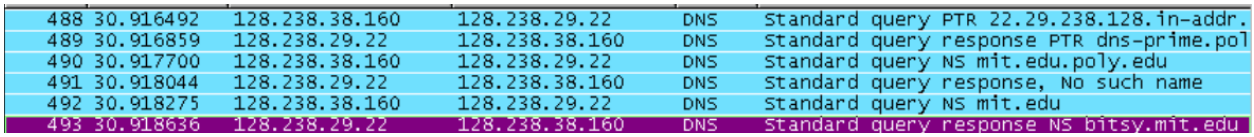
these answers contain? (Hint: Consider packets similar to the yellow highlights portion of the screenshot. You will not see responses for packets that say “No such name A www.mit.edu” in the “Info” tab of the Wireshark tool.)

Answers

www.mit.edu: type A, class IN, addr 18.7.22.83

Name: www.mit.edu
Type: A (Host
address) Class:
IN (0x0001)
Time to live: 1 minute
Data length: 4
Addr: 18.7.22.83

14. Provide a screenshot



488	30.916492	128.238.38.160	128.238.29.22	DNS	Standard query PTR 22.29.238.128.in-addr.
489	30.916859	128.238.29.22	128.238.38.160	DNS	Standard query response PTR dns-prime.pol
490	30.917700	128.238.38.160	128.238.29.22	DNS	Standard query NS mit.edu.poly.edu
491	30.918044	128.238.29.22	128.238.38.160	DNS	Standard query response, No such name
492	30.918275	128.238.38.160	128.238.29.22	DNS	Standard query NS mit.edu
493	30.918636	128.238.29.22	128.238.38.160	DNS	Standard query response NS bitsy.mit.edu

15. To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?

It was sent to 128.238.29.22 which is the default DNS server.

16. Examine the DNS query message. What “Type” of DNS query is it? Does the query message containing any “answers”?

The type of DNS query is an NS DNS query which doesn’t contain any answers.

17. 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?

The nameservers that the MIT response message is w20ns, strawb, and bitsy. Yes, the response message also provides the IP addresses of the MIT nameservers.
Addr 18.72.0.3
Addr 18.71.0.151
Addr .18.70.0.160