In class Lab DNS and nslookup (dig in Mac)

Purpose: To understand in more details the DNS process and what happens during DNS query.

Learning Activities: At the end of these activities, you should understand how DNS and other online databases allow the internet to work.

Reflect on this question at the end of the lab: An attacker managed to set themselves as your gateway, how can they modify DNS settings for your host?

Download the Wireshark file “DNS” in the Canvas extra credits section, and open it up in Wireshark.

Answer the following questions. Once you complete it, check your answers with one of your class mates.

* Which is the domain being searched for?
  + Intel.com
* Which are the IP addresses of the domain being searched for?
* The first request is of class of PTR. What is the PTR?
  + Domain name pointer
* The second request is of class for A. What is the A class?
  + Host address
* The last request is for class of AAAA. What is the AAAA class?
  + IN(0x0001)
* Does the domain have an IPv6 address?
  + Yes

Using nslookup or dig, determine the main **IP addresses** for the following **domains:**

1. Xavier.edu
   1. 209.87.149.24
   2. 209.87.150.139
2. Facebook.com
   1. 157.240.18.35
3. Intel.com
   1. 13.91.95.74
4. hackerrank.com
   1. 34.201.232.161

Using nslookup or dig and using type=soa and type=mx, for Cisco.com, determine the following: For **Mac** use this command dig @8.8.8.8 +nocmd +multiline +noall +answer any cisco.com SOA. For **Windows** use this command: nslookup -type=MX CISCO.com

* Primary name server:
  + ns1.cisco.com
* Serial number of record:
  + 21049453
* Refresh time:
  + 7200
* Retry:
  + 1800
* Expire time:
  + 864000
* Default TTL:
* Name servers:
* Mail servers (and their preference value):
  + postmaster.CISCO.com
* IP Address of mail servers:
* What security risk is there involved with these records?
  + Everything is public that we can see.