Quiz 4 DNS quiz student name: Evan Smith

1:10 what is DNS, why do we need DNS? How does it work?

DNS is the Domain Name System, which links human readable domains to IP addresses. We need this to allow us to easily navigate with meaningful handles to addresses. It moves through several servers in order to look up the appropriate IP address to send the traffic to.

2: 10 how does DNS do its query? What does it check the first, and second etc.?

First, it goes through the recursor to the root nameserver. This narrows the search, and then checks the TLD nameserver, which is where the sites with that suffix (ie .com) are stored. Finally, it looks at the authoritative nameserver which returns the matching IP address, if it exists.

3: 10 what is DNS cache? What is it for?

The DNS cache stores previously discovered DNS entries locally to speed up the process of resolving domain names to IPs.

4: 15 what is DNS cache poison?  
This is when the cache is attacked and the stored domains are remapped to meaningless or incorrect IP addresses.

5:15 what are necessary for your spoofed packet in order to successfully spoof attack the DNS?

You must be able to send a request and response nearly simultaneously such that it appears to the DNS server that the request for a domain and the answer from the authoritative source both appear at the correct time. You must also sign your spoofed packet such that it appears authoritative in UDP.

6: 15 challenges for DNS cache poison? Reasons?

You must be fast in order to beat the actual authoritative response. Additionally, the fake request must be an uncached domain in order to trigger a lookup, and the request ID must be in the correct sequence.

7: 15 what is Kaminsky attack (detail)?

The idea is that while it is very difficult to carry out the attack in a single try, like it would take for a single domain, you can use a random value as the beginning of the domain with the rest the same, creating a sibling domain that will trigger a lookup. This allowed for a spoofed reply to have the right TID within a matter of minutes rather than months.

8: 10 what is Denial-of-Service on DNS servers?

DoS attacks are a flooding of traffic to servers such that it fills their work queue and blocks the processing of legitimate traffic. This is often done using botnets that have very high bandwidth to increase the volume of traffic even more.