Quiz 4 DNS quiz student name: Kevin Martin

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

DNS is domain name system, and it is a system that converts a domain name to an IP address and vice versa.

We need DNS because it allows humans to not have to remember each IP address of the website they wish to visit while also allowing for allowing computers to use the complicated IP address protocol.

It works by a using a distributed approach (as opposed to a centralized approach) whereby a **structure** is put in place that allows a request for a specifc IP address to be routed to the correct machine which knows the "answer". This is a hierarchical structure, organzied as a tree. DNS does its query by entering the hierarchical/tree structure at the root (root server). The query passes through each layers to find its ultimate answer.

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

The user machine queries its local DNS server, which will then find a way to get the answer for the user.

DNS does its query by entering the hierarchical/tree structure at the root (root server). The query passes through each layers in an iterative approach to find its ultimate answer.

The DNS query first checks the Top-Levle Domain (TLD) which is the website suffix, such as .com, .net, .uk, etc.

Next, the DNS query checks is the domain name, which is the name of the address that is bought/owned by the owener (such as apple or micorosoft).

After that, the zone is checked, because different zones for a given domain are hosted by different servers and this needs to be checked.

Finally, the result will be cached by the local DNS server

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

DNS cache is local DNS machine's previously saved DNS query requests. So if the address was recently queried, the local machine does not need to send another request.

It is a static mapping between the domain name and the IP address, and is used to reduce the number of query requests from a local machine.

4: 15 what is DNS cache poison?

A malicious server returns false IP addresses in the "Additional Section" of a DNS reqeust. This would force the user to connect to those falsely provided IP addresses for the duration specified by the attacker (as the response packet indicates the length of time that these IP addresses stay in the user's cache).

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

The necessary items for a successfully spoofed packet are: the source IP, destination IP, source port, destination port, and transaction ID.

6: 15 challenges for DNS cache poison? Reasons?

The challenges for DNS cache poisoning are the gathering the desintation port and transactoin ID. These are 32 bit numbers so there are 2^{32} possible numbers to try to guess. If the guess is incorrect, the malicious packet is dropped, which allows the real packet to be returned and accepted, thus cacheing the domain name and correct IP address. This means the cache poisoning attack was generally limited to attacks from the local network.

7: 15 what is Kaminsky attack (detail)?

The Kaminsky attack solves the cache effect problem by providing fake information in the Authority section. This section holds information about the namespace. Random names are used to avoid being blocked by the cache effect. Eventually, the attacker will get lucky with getting the transaction ID and port number, and thus the information will be cached.

When the user tries to access a specific namespace, the cache will point the user to the attacker’s server.

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

A DOS on DNS attack is one that targets a specific DNS server, generally a layer or two beneath the root, with the intention of preventing that server from fulfilling any incoming requests.