**Assessment 1c-Bi-Weekly (week5-6)**

# Question 1

The domain name service (DNS) is a service component that provides the translation of an actual IP address to a name or vice versa, enabling computers to locate devices connected to a network. It uses the client-server mechanism in which clients input URLs into the web browser for host address information. The DNS maintains a database consisting of information of hosts within a specific zone, where every zone must include the authoritative name server containing information about all hosts it supports in that particular zone (Novell,2019). The DNS name server itself is split into two parts: primary name server and secondary name server

Besides maintaining local host information, DNS maintains information about how to establish connection with other name servers in an internetwork. The name servers in an internetwork try to retrieve host information and initiate a connection between each other. However, if the DNS doesn’t have information about a particular domain, the name server repetitively forward requests to domains up or down the domain hierarchy until an authoritative answers isn’t received for the client’s query

As aforementioned above, there are two types of name servers namely primary and secondary name servers where, different types of domain data are stored in each name server

## Primary Name Server

The primary name server holds hostname and address information in an authoritative database for an entire domain within the administrative zone. The domain administrator updates the database whenever any changes occur.

## Secondary Name Server

The secondary name server only holds copies of the primary name server database. These servers are responsible for load balancing and providing redundancy for a domain. Whenever, the secondary name server starts, it requests a full copy of the primary DNS server database which is also known as the process of zone transfer. if needed, the primary name server can also work as a secondary name server too.

Furthermore, both the name servers maintain the DNS database containing address and hostname information in the form of resource records. There are many types of resources records that maintain different type of host information. Some types of resource records are mentioned below

* Start of authority= start of authority for a zone
* Address (A)= the IP address for the specific zone
* Canonical Name (CNAME)= primary name of owner, where owner name is an alias

# Question 2

DNS cache poisoning also known as DNS spoofing is a type of cyber-attack in which an intruder diverts internet traffic away from genuine servers towards malicious ones. Every internet service provider has their own DNS servers which have a cache of information from other DNS servers. The local computer also has a DNS cache to perform faster DNS lookups already done previously, besides performing the DNS lookups repetitively. The DNS cache is said to be poisoned when a malicious entry is made by the attacker in the cache.

For instance, if the intruder gets hold of the DNS server, the attacker can change the information (Hoffman, C, 2016). If a client requests a site such as “stackoverflow.com”, the attacker can point the client towards his own server. Moreover, DNS cache poisoning can be extremely dangerous since a poisoned entry on any legitimate server and been sent out to internet service providers will be stored in their cache. This would enhance the effect by further spreading to home computers and routers, as a result, having their local cache poisoned.

The solution to DNS cache poisoning is through the implementation of DNSSEC that adds a top authentication layer on DNS (CloudFare, 2014). The DNNSEC works by adding cryptographic signatures over DNS records. These digital cryptographic signatures are stored in name servers on records such as A, AAA, and several others. The digital signature provides a way to verify that the requested DNS records comes from the authoritative name server and wasn’t altered, as would it be in a man-in-the-middle attack. The DNSSEC adds the following signatures on the DNS records

* RRSIG= contains the digital cryptographic signature
* DNSKEY= the public signed key
* DS= hashing value of the DNSKEY
* NSEC=
* CDNSKEY= child zone requesting updates to DS records

# References

* *Cloudflare, How DNSSEC Works (2014). Cloudflare. [online] Cloudflare. Available at:* [*https://www.cloudflare.com/dns/dnssec/how-dnssec-works/*](https://www.cloudflare.com/dns/dnssec/how-dnssec-works/)*.*
* *‌Hoffman, C. (2016). What is DNS Cache Poisoning? [online] How-To Geek. Available at:* [*https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/*](https://www.howtogeek.com/161808/htg-explains-what-is-dns-cache-poisoning/)*.*
* *Novell.com. (2019). Novell Documentation. [online] Available at:* [*https://www.novell.com/documentation/dns\_dhcp/?page=/documentation/dns\_dhcp/dhcp\_enu/data/behdbhhj.html*](https://www.novell.com/documentation/dns_dhcp/?page=/documentation/dns_dhcp/dhcp_enu/data/behdbhhj.html)***.***