Name :- Asjid Jahir

Roll no :- 19p-0085

Course :- Computer Networks

Class Activity (1) :-

i) types of DNS servers :-

following are the three type of DNS servers :-

↳ DNS resolver :

↳ It is design to recieve one queue.

↳ It is responsible for hacking Internet prodocol (Ip) for host names.

↳ DNS root server :

↳ It extends the top level domain from users query.

www. google

↳ provides details for (.com).

TLD (Name Server)

↳ TLD Name Servers:

↳ maintains information for all domain names that share common domain extension.

↳ e.g .net, .com etc.

↳ Authoritative Name Servers:-

↳ In this, DNS server in the authoritative server for specific host name, basically it holds up to date informed for host name.

ii) What kind of information stored in DNS:-

↳ DNS stored information about:

↳ Ip addresses associated with domain.

↳ Domain name.

↳ Handling request.

↳ series of text files written in form called DNS records.

iii) what type of handle zone transfer & information could possibly stored ?

↳ DNS handles zone transfer and name servers has DNS information of all URLs with that name's servers domain.

↳ DNS server stores domain names with corresponding identifier called Ip addresses.

↳ It stores cache that save your time when you revisit that website.

iv) Importance of DNS & information stored on it :-

↳ DNS is most important because it stores Ip addresses relevent to URL.

↳ ~~Information~~ It is important and professional for all domains to have a specific set of default records or cache.

↳ Records that stored in authoritative servers provides information about domains.

v) Why it is ideal for an organization to have more than one name sever?

↳ For organization with multiple websites, which often have similar content, its common to have domains spread across multiple hosts and have more than one name sever.

↳ With have multiple DNS, the load on primary DNS reduced and hence customers get more seamless experience.

vi) Dangerous to transfer information without checking client.

↳ It is very dangerous to transfer information without checking client because they may be attackers which may install malware on users system and change the local DNS setting to the milicious sites.

vii) Why do you think should be done to prevent such things?

↳ DNS is highly sensitive infa-structure that requires strong security measures, one should do:

- Watch for resolvers on your network.
- Severly restrict access to name server.
- Take action against cache poisoning.
- Restrict zone transfer.
- Separate authoriative name servers from resolvers.