DNS Zone Transfer

What are DNS Zone Transfers ?

A DNS zone transfer is a process where a portion of a DNS server's database, which called a **"zone"**, is copied to another DNS server. This is done for redundancy and reliability purposes.

Imagine you have a company website example.com. The DNS server that has the master copy of the example.com zone is called the primary DNS server. To ensure the website stays online even if the primary server goes down, you have secondary DNS servers that keep copies of the zone.When changes are made to the example.com zone on the primary server, those changes need to be copied to the secondary servers. This is where zone transfers come in:

1. The primary server has the "master copy" of the example.com zone.
2. The secondary servers periodically check the primary server to see if the zone has changed by comparing serial numbers.
3. If the zone has changed (higher serial number), the secondary server will request a zone transfer from the primary to get the updated zone data.
4. The primary server will send over the entire zone file to the secondary server, allowing it to keep its copy up-to-date.

Now the problem arises when the primary server is misconfigured to allow zone transfers to any server that requests it, not just the authorized secondaries. This allows anyone on the internet to request and obtain the zone data, which can contain sensitive information like server names, email addresses, and IP addresses.

Lets see how we can perform zone transfer.

DNS Zone transfer with dnsenum, dnsrecon & dig

```
dig axfr <domain> @Primary/Secondary Name Server

dnsenum <domain>

dnsrecon -d <domain>
dnsrecon -d <domain> -t axfr
```

So to summarize this, zone transfers are a normal part of DNS, but misconfigured servers can expose sensitive data. Proper security measures should be taken to restrict zone transfers to only authorized servers.
