DNS recon using host, nslookup and dig

As we all know, DNS is a critical component of the internet infrastructure, responsible for translating human-readable domain names into machine-readable IP addresses. During the reconnaissance phase of web application security assessments, understanding and gathering information about a target's DNS setup can provide valuable insights.

Before going into the recon techniques, lets understand DNS records first.

Each domain can use different types of DNS records. Some of the most common types of DNS records include:

- **NS**: Nameserver records contain the name of the authoritative servers hosting the DNS records for a domain.
- **A**: Also known as a host record, the "*a record*" contains the IPv4 address of a hostname (such as www.example.com).
- **AAAA**: Also known as a quad A host record, the "*aaaa record*" contains the IPv6 address of a hostname (such as www.example.com).
- **MX**: Mail Exchange records contain the names of the servers responsible for handling email for the domain. A domain can contain multiple MX records.
- **PTR**: Pointer Records are used in reverse lookup zones and can find the records associated with an IP address.
- **CNAME**: Canonical Name Records are used to create aliases for other host records.
- **TXT**: Text records can contain any arbitrary data and be used for various purposes, such as domain ownership verification.

Let's look into the recon techniques now. We will start off with the host command.

DNS Recon using Host

host is a command-line tool for converting domain names to IP addresses and vice versa. It can also be used to perform reverse lookups, list DNS records, and check for zone transfers

```
host tipsbangalore.com - resolves & find IP address
host -t ns <domain> - Shows Nameservers
host -t mx <domain> - Shows MailServers
host <IP> - Reverse DNS Lookup
```

DNS Recon with nslookup

NSlookup is an interactive tool for querying DNS servers, mapping domain names to IP addresses, and retrieving DNS records. Great thing is that, it works on both Linux and Windows.

```
nslookup <domain> -> Find IP address

nslookup -> Find NS records
set type=ns
<domain>

set type=mx -> Find MX records
<domain>
```

DNS Recon with dig

dig is a very flexible tool for interrogating DNS name servers, with advanced features for performing complex queries.

```
dig <domain>


dig <domain> -t mx -> The lowest number indicates the server with the
highest priority

dig <domain> -t ns
dig <domain> AAAA
dig <domain> CNAME
```

A CNAME record is like a nickname or alias for a domain name. It allows you to point one domain or subdomain to another domain.For example, let's say you have a website at example.com. You can create a CNAME record to make www.example.com point to example.com. This way, both the root domain (example.com) and the www subdomain (www.example.com) will go to the same website.
