Class: an encoded 16-bit value that identifies a protocol family or instance of a protocol

IN: The Internet system

CH: The Chaos system

TTL: The time to live of the RR. The TTL describes how long a RR can be cached before it should be discarded.

RDATA: The type-dependent and sometimes class-dependent data that describes the resource

DNS Queries There are five types of queries that can be carried out on a WHOIS database:

1. Registrar: Displays specific registrar information and associated WHOIS servers. It provides details about the potential domains that correlate to the target.

2. Organizational: Displays all information related to a particular organization. This query can list all known instances associated with the particular target and the number of domains associated with the organization.

3. Domain: Provides information about a specific domain. A domain query arises from information gathered from an organizational query. An attacker can use a domain query to find the address, domain name, phone number of the administrator, and the system domain servers of the company.

4. Network: Provides information about a network with one IP address. Network enumeration can help ascertain the network block assigned or allotted to the domain.

5. Point of contact (POC): Displays information about personnel that deal with administrative, technical, or billing accounts.

If an organization is a high-security organization, it can opt to register a domain in the name of a third party, as long as that party agrees to accept responsibility. The organization must also take care to keep its public data updated and relevant for faster resolution of any administrative or technical issues. The public data is available only to the organization that is performing the registration, and that entity is responsible for keeping it current.

DNS Record Manipulation DNS servers cache recent data for fast retrieval. DNS poisoning involves damaging a server’s DNS table. Using this technique, an attacker replaces the IP address of a system with the address of a system owned by the attacker. Then, worms, viruses, and other malware programs can be downloaded onto the user’s system, or the attacker can steal the user’s personal information.

Defending against DNS Attacks The first line of defense for any target system is proper configuration and implementation of its DNS. The system must refuse inappropriate queries, thereby blocking crucial information leakage.

Another best practice is to use more than one DNS, where one DNS caters to the external interface, and the other to the internal interface. This lets the internal DNS act like a proxy server, thus shielding the internal servers from leaking information to the outside.

Tool: Nslookup

Nslookup is a valuable tool for querying DNS information for host name resolution. It is bundled with both UNIX and Windows and is accessed from the command prompt. When a user runs Nslookup, it shows the host name and IP address of the DNS server that is configured for the local system, and then it displays a command prompt for further queries. This is the interactive mode. Interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain.

Noninteractive mode is used to print the name and requested information for a host or domain.

Nslookup allows the local machine to use a DNS server that is different from the default one by invoking the server command. By typing server <name> (where <name> is the host name or IP address of the server the user wants to use for future lookups), the system uses the given DNS server. The following is an example of Nslookup:

```
slookup
Default Server: cracker.com
Address: 10.11.122.133
Server 10.12.133.144
```