nslookup

What is nslookup?

Nslookup is the name of a program that lets users enter a <u>host</u> name and find out the corresponding <u>IP address</u> or domain name system (<u>DNS</u>) record. Users can also enter a command in nslookup to do a reverse DNS lookup and find the host name for a specified IP address.

Uses for nslookup

Network administrators use nslookup to <u>troubleshoot server connections</u> or for security reasons. For example, network pros might use nslookup to guard against <u>phishing</u> attacks, in which attackers alter domain names. An attacker might substitute the numeral *1* for a lowercase *l* to make an unfriendly site look friendly and familiar, e.g., *joes1owerprices.com* vs. *joeslowerprices.com*. Network admins use nslookup to troubleshoot such attacks.

DNS, or nslookup, also helps deter <u>cache poisoning</u>, in which attackers distribute data to caching resolvers that pose as authoritative origin servers.

Examples of nslookup commands

Popular nslookup commands include the following:

- `/name` -- queries the current name server for the specified name.

- `/server name` -- sets the current name server to the server the user specifies.

- `/root` -- sets the root server as the current server.

- `/set type=x` -- specifies the type of records to be displayed, such as A, <u>CNAME</u>, MX, NS, PTR or SOA. Specify ANY to display all records.

- `/set debug` -- turns on debug mode, which displays detailed information about each query.

- `/set recurse` -- tells the DNS name server to query other servers if it does not have the information.

- `/exit` -- exits nslookup and returns the user to a command prompt.

Nslookup has two modes: interactive and noninteractive. To look up only a single piece of data, use noninteractive mode. To look up more than one piece of data, use interactive mode.

Nslookup sends a domain name query packet to a designated -- or defaulted -- DNS server. Based on the system used, the default could be the local DNS server at the service provider, some intermediate name server or the root server system for the entire DNS hierarchy.

```
nslookup <domainName>
```