Nslookup Command

Objective:

Learn how to use the Nslookup command to gather DNS information on a target site.

Purpose:

Nslookup is a network administration command-line tool used for querying the DNS to obtain domain name or IP address mapping information.

Tool:

Windows Machine or Kali Linux.

Topology:

You can use a Windows Machine or Kali Linux for this lab.

Walkthrough:

Task 1:

Nslookup comes built in on both Windows and Linux. In Windows, it comes in both an interactive and non-interactive mode. To open the interactive mode, type “nslookup”. To quit the interactive mode, type “quit”.

We will begin by finding the IP address of a host. To do this, type the following:

nslookup www.google.com

```
Microsoft Windows [Version 10.0.19045.5011]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ALL AtoZ>nslookup www.google.com
DNS request timed out.
    timeout was 2 seconds.
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
Name:    www.google.com
Addresses:  2a00:1450:400e:811::2004
          216.58.223.196


C:\Users\ALL AtoZ>
```

As you will see, we are returned with the different IPv4 and IPv6 ip addresses for Google.com. The node, called as “local DNS resolver”, is the first point of contact we make with a DNS query every time.

This is usually the IP address of the device provided to you by your Internet Service Provider. Of course, you can target your “all DNS queries” to a different server by changing your local machine’s network settings accordingly.

Task 2:

We will now perform a reverse lookup which will match an IP address to a domain name. This is also called the DNS PTR record, and can be thought of as the exact opposite of the DNS A record. To do this type:

nslookup 74.125.193.99

```
C:\Users\ALL AtoZ>nslookup 216.58.223.196
Server:  UnKnown
Address:  172.20.10.1

Name:    los02s03-in-f4.1e100.net
Address:  216.58.223.196
```

Oftentimes, we can see that hostnames DNS A and DNS PTR queries do not match on web servers. This is because multiple IP addresses may be matched against a DNS A record to perform load balancing.

Task 3:

We can also find any “Mail eXchange” servers for a particular domain. To do this, type:

nslookup -querytype=mx google.com

```
C:\Users\ALL AtoZ>nslookup -querytype=mx google.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
google.com      MX preference = 10, mail exchanger = smtp.google.com
```

Task 4:

We can also find the “Name Servers” responsible for a domain. In other words, only those servers which are authoritative sources to keep DNS records of the google.com domain name. To do this, first open an interactive console by typing “nslookup”. Then, type:

set query=ns

Then, type the domain name into the terminal.

```
C:\Users\ALL AtoZ>nslookup
Default Server:  UnKnown
Address:  172.20.10.1

> set query-ns
> set query=ns
> google.com
Server:  UnKnown
Address:  172.20.10.1

Non-authoritative answer:
google.com      nameserver = ns4.google.com
google.com      nameserver = ns3.google.com
google.com      nameserver = ns1.google.com
google.com      nameserver = ns2.google.com
>
```

Task 5:

It is possible to access domain verification data by making a DNS TXT query.

nslookup -querytype=txt google.com

```
Non-authoritative answer:
google.com      text =

        "google-site-verification=wD8N7i1JTNTkezJ49swvWW48f8_9xveREV4oB-0Hf5o"
google.com      text =

        "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com      text =

        "v=spf1 include:_spf.google.com ~all"
google.com      text =

        "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com      text =

        "cisco-ci-domain-verification=479146de172eb01ddee38b1a455ab9e8bb51542ddd7f1fa298557dfa7b22d963"
google.com      text =

        "google-site-verification=4ibFUgB-wXLQ_S7vsXVomSTVamuOXBiVAzpR5IZ87D0"
google.com      text =

        "google-site-verification=TV9-DBe4R80X4v0M4U_bd_J9cpOJM0nikft0jAgjmsQ"
google.com      text =

        "MS=E4A68B9AB2BB9670BCE15412F62916164C0B20BB"
google.com      text =

        "apple-domain-verification=30afIBcvSuDV2PLX"
google.com      text =
```