

# Lab 16 – Nslookup Command

Lab Objective:

Use the Nslookup command to gather DNS information on a target site.

Lab Purpose:

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

Lab Tool:

Windows Machine or Kali Linux.

Lab Topology:

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

Lab Walkthrough:

## Task 1: Finding the IP Address of a Host (A Record)

Essence & Purpose:

The primary purpose of this task is to **resolve a domain name to an IP address**, which is the foundation of internet communication.

- **Logic:** When you type a domain like [www.google.com](http://www.google.com), the internet doesn't understand domain names directly. Instead, it works with **IP addresses**. Therefore, the **DNS (Domain Name System)** translates human-readable domain names into machine-readable IP addresses.
- **Purpose:** This query helps you discover which **IPv4 and/or IPv6 addresses** correspond to the domain you're querying. This is critical because all internet communications, such as browsing websites, rely on these IP addresses to locate and connect to web servers.
- **Example:** When you look up [google.com](http://google.com), you are shown multiple **IP addresses** because Google may have multiple servers handling requests across different regions for **load balancing** and **availability**.

Run:

nslookup google.com

```
(femi@KALI)-[~]-
$ nslookup www.google.com
Server:      192.168.1.1
Address:     192.168.1.1#53

Non-authoritative answer:
Name:   www.google.com
Address: 216.58.223.228
Name:   www.google.com
Address: 2c0f:fb50:4003:602::2004

(femi@KALI)-[~]-
$
```

## Task 2: Performing a Reverse Lookup (PTR Record)

### Essence & Purpose:

This task demonstrates the ability to **reverse the process** of resolving an IP address back to a domain name.

- **Logic:** The **reverse lookup** (PTR record) works similarly to a forward lookup but does the opposite. It's useful when you want to identify the **hostname** of an IP address. This is especially important for network diagnostics, security, and email validation.
- **Purpose:** Reverse lookups are often used for **tracing IPs** back to their domain names in activities like identifying the owner of an IP address, checking if an email is coming from a legitimate source (to combat spam), or identifying network misconfigurations.
- **Example:** Performing a reverse lookup for an IP address like **74.125.193.99** returns a domain name (**ord38s02-in-f3.1e100.net**). This helps in verifying the origin or ownership of the IP address.

## Nslookup “ip address”

### Essence & Purpose:

- **Logic:** Email communication on the internet doesn't use the domain name directly. Instead, it relies on **MX records**, which direct email to the appropriate mail servers for the domain. Each MX record also has a **priority number**, which helps to decide which server to contact first.

- ```
nslookup -querytype=mx funaab.edu.ng
```

[illegible]

---

## Task 4: Querying Name Servers (NS)

### Essence & Purpose:

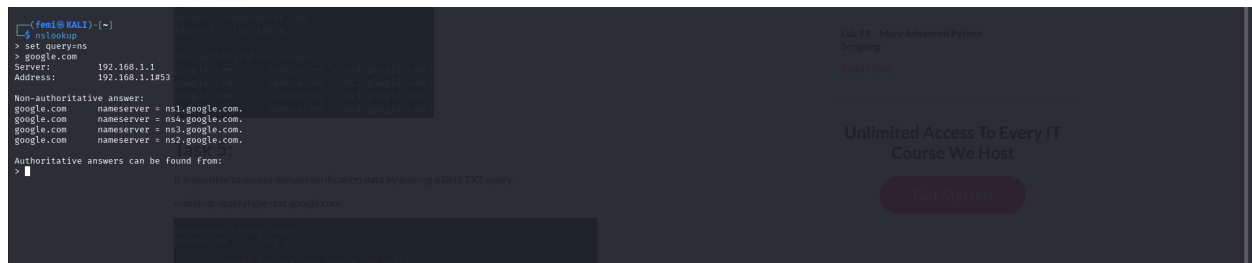
This task focuses on retrieving the **authoritative DNS servers (NS records)** for a domain, which are responsible for maintaining and providing DNS information.

- **Logic:** Every domain has **Name Servers** that hold the DNS records (like A, MX, etc.). When a DNS query is made, the authoritative Name Servers for the domain provide the requested information. These servers are **authoritative**, meaning they are the **source of truth** for that domain's DNS records.
- **Purpose:** By identifying the **authoritative name servers**, you can:
  - Understand where DNS records for a domain are managed.
  - Troubleshoot DNS resolution issues.
  - Investigate how DNS is set up for a domain or verify its configuration.
- **Example:** By querying **google.com**, you can find out which servers are responsible for maintaining the DNS records for Google. This is important for troubleshooting DNS issues or confirming domain ownership.

Run:

Nslookup

Then input the website; e.g google.com



```
(femi@KALI)-[~]
$ nslookup
> set querytype
> google.com
Server:      192.168.1.1
Address:     192.168.1.1#53

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

Authoritative answers can be found from:
>
```

On the right side of the terminal window, there is a sidebar with the text: "Get 15+ More Advanced Python Scripts" and "Unlimited Access To Every IT Course We Host".

## Task 5: Querying DNS TXT Records

### Essence & Purpose:

This task involves querying **TXT records**, which store arbitrary text data, including crucial information like **email security settings** (SPF, DKIM) and domain verification data.

- **Logic:** **TXT records** can store any text string. Common uses include:
  - **SPF records** (Sender Policy Framework): A type of TXT record used to define which mail servers are allowed to send emails on behalf of the domain (helpful for email security).
  - **Domain verification:** Some services require TXT records for domain ownership verification (e.g., Google Search Console).
- **Purpose:** By querying TXT records, you can:
  - Access **email security settings** to prevent spoofing and phishing attacks (via SPF).
  - Verify domain ownership for services like email or cloud applications.
  - Obtain additional textual information about the domain's DNS setup.
- **Example:** By querying `google.com` for TXT records, you might find information like the **SPF record** (`v=spf1 include:_spf.google.com ~all`), which helps prevent unauthorized servers from sending email that appears to be from Google.

Run:

```
nslookup -querytype=txt google.com
```

```
nslookup -querytype=txt funaab.edu.ng
```

```
File Actions Edit View Help
Address: 172.158.1.100
Non-authoritative answer:
Name: google.com
Address: 172.158.1.100
Authoritative answers can be found from:
Name: google.com
Address: 172.158.1.100
Task 2:
nslookup google.com
Server: 172.158.1.100
Address: 172.158.1.100
Non-authoritative answer:
Name: google.com
Address: 172.158.1.100
Authoritative answers can be found from:
Name: google.com
Address: 172.158.1.100
Task 3:
nslookup google.com
Server: 172.158.1.100
Address: 172.158.1.100
Non-authoritative answer:
Name: google.com
Address: 172.158.1.100
Authoritative answers can be found from:
Name: google.com
Address: 172.158.1.100
```

Summary of the Overall Purpose of nslookup:

- 1. **DNS Resolution:** The main purpose of nslookup is to help resolve domain names into IP addresses and vice versa, allowing devices to communicate over the internet.
- 2. **DNS Troubleshooting:** By querying different types of records (A, PTR, MX, NS, TXT), nslookup is essential for troubleshooting network and DNS issues, such as identifying why a website is down, where emails are being routed, or who controls a domain.
- 3. **Security:** DNS-related queries (like MX and TXT) are also used for security purposes, including verifying mail servers and setting up email security protocols like SPF to prevent malicious activities.

In summary, each task allows you to query different DNS records, each serving a specific function—whether for identifying domain names, troubleshooting DNS issues, or securing email communication. Understanding how to use nslookup in these various ways is foundational for network and security professionals.