

Project Title: DNS Reconnaissance and Analysis Using `nslookup`

Objective

To demonstrate proficiency in using `nslookup` for DNS querying tasks, including A/MX/NS record retrieval, server-specific lookups, and interactive analysis. The goal is to build core DNS troubleshooting skills, foundational to IT support and security operations (SOC) for detecting misconfigurations, malicious redirections, and verifying domain integrity.





Tools Used

- **OS Environment:** Kali Linux / Ubuntu / Windows (cross-platform)
- **Primary Utility:** `nslookup`
- **DNS Servers Queried:** Default resolver, Google DNS (8.8.8.8), custom as needed

Skills Learned

- Understanding DNS resolution flow (local → recursive → authoritative)
- Differentiating between A, MX, and NS records
- Using specific DNS servers to test external resolution behavior
- Discovering domain hierarchy and registrar details
- Operating in interactive vs. non-interactive modes of DNS tools
- Diagnosing DNS poisoning or misrouting issues

Test Scenarios Executed

Level	Task Description	Sample Command
 Basic	Find the IP address (A record) of a domain	<code>nslookup example.com</code>
 Intermediate	Query a specific DNS server (Google Public DNS) for the domain's resolution	<code>nslookup example.com 8.8.8.8</code>
 Advanced	Use interactive mode to query multiple record types (e.g., A and MX for openai.com)	<code>nslookup → set type=A / set type=MX → openai.com</code>
 Advanced	Retrieve NS records to view authoritative servers and understand domain delegation hierarchy	<code>nslookup -type=NS openai.com</code>

Real-World Impact & Use Case

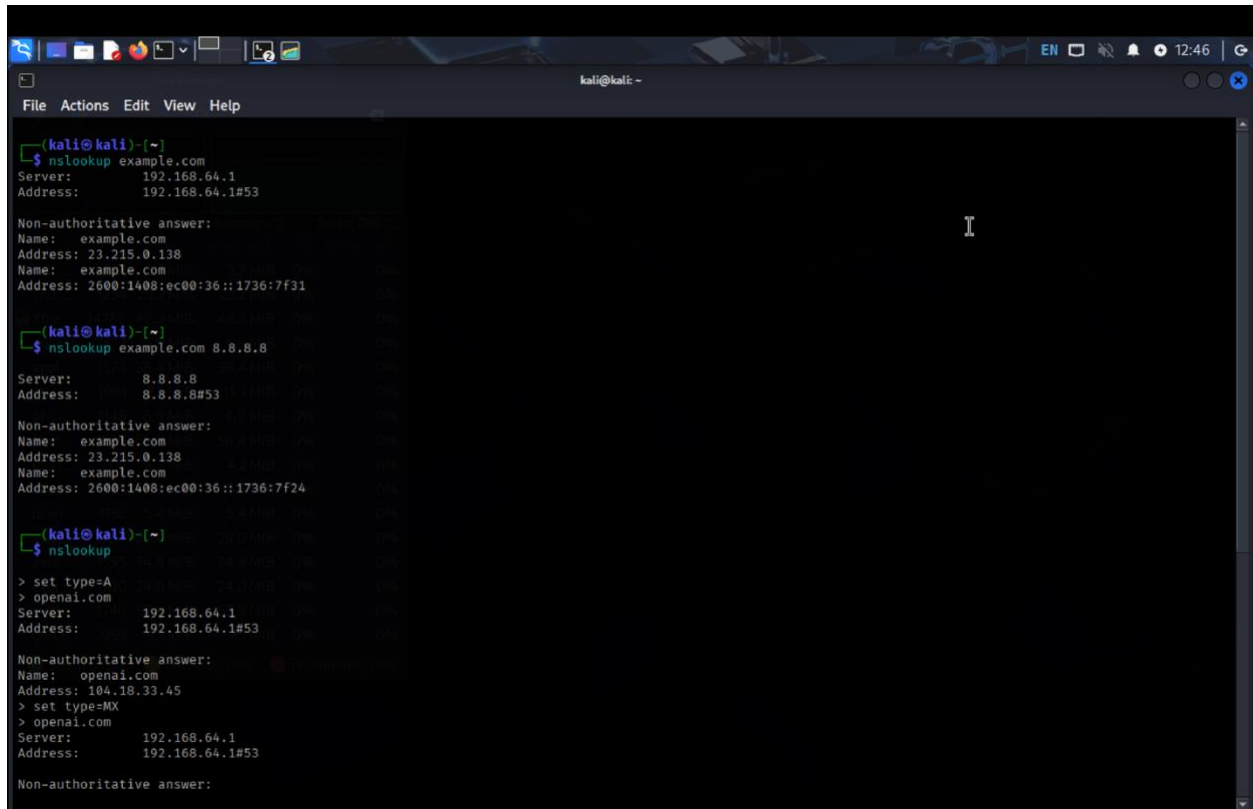
For IT professionals and SOC analysts, `nslookup` is an essential command-line tool for:

- Verifying DNS propagation after domain updates
- Diagnosing email delivery failures (MX record validation)
- Checking for DNS spoofing or hijacking
- Evaluating DNS server responsiveness and redundancy

- Supporting compliance audits by validating DNS configurations
- Forensics and threat intel analysis (e.g., identifying suspicious name servers)

Bonus Insight (SOC Use Case)

- Attackers often exploit DNS to redirect users to phishing sites. By using `nslookup` on suspected domains and comparing results across DNS servers, analysts can **detect DNS poisoning or unauthorized record changes** — a critical investigative technique in cyber defense.
-



```
(kali@kali)-[~]
$ nslookup example.com
Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f31

(kali@kali)-[~]
$ nslookup example.com 8.8.8.8
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   example.com
Address: 23.215.0.138
Name:   example.com
Address: 2600:1408:ec00:36::1736:7f24

(kali@kali)-[~]
$ nslookup
> set type=A
> openai.com
Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
Name:   openai.com
Address: 104.18.33.45
> set type=MX
> openai.com
Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
```

```
(kali@kali)-[~]
$ nslookup

> set type=A
> openai.com
Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
Name:   openai.com
Address: 104.18.33.45
> set type=MX
> openai.com
Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
openai.com mail exchanger = 10 alt3.aspmx.l.google.com.
openai.com mail exchanger = 5 alt2.aspmx.l.google.com.
openai.com mail exchanger = 10 alt4.aspmx.l.google.com.
openai.com mail exchanger = 1 aspmx.l.google.com.
openai.com mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
> exit

(kali@kali)-[~]
$ nslookup -type=NS example.com

Server:      192.168.64.1
Address:     192.168.64.1#53

Non-authoritative answer:
example.com nameserver = a.iana-servers.net.
example.com nameserver = b.iana-servers.net.

Authoritative answers can be found from:

(kali@kali)-[~]
$
```