**🌐 nslookup – Ultimate Cheat Sheet**

**🔹 1. Basics**

**Syntax**

nslookup [options] [domain/ip] [server]

**Example**

nslookup example.com

**🔹 2. Interactive Mode**

Start interactive shell:

nslookup

Inside interactive mode:

* server 8.8.8.8 → use specific DNS server
* set type=A → query A records
* set type=MX → query mail servers
* set type=NS → query nameservers
* exit → leave interactive mode

**🔹 3. Common Queries**

| **Record Type** | **Command Example** | **Description** |
| --- | --- | --- |
| A (IPv4) | nslookup -type=A example.com | Get IPv4 address |
| AAAA (IPv6) | nslookup -type=AAAA example.com | Get IPv6 address |
| MX | nslookup -type=MX example.com | Get mail servers |
| NS | nslookup -type=NS example.com | Get nameservers |
| TXT | nslookup -type=TXT example.com | Get SPF/DKIM/verification |
| SOA | nslookup -type=SOA example.com | Get zone authority info |
| CNAME | nslookup -type=CNAME www.example.com | Get alias mapping |
| PTR | nslookup 8.8.8.8 | Reverse DNS lookup |

**🔹 4. Using Specific DNS Server**

Query Google DNS:

nslookup example.com 8.8.8.8

Query Cloudflare DNS:

nslookup example.com 1.1.1.1

**🔹 5. Advanced Options**

| **Command** | **Description** |
| --- | --- |
| set port=5353 | Use custom port |
| set timeout=10 | Set timeout in seconds |
| set debug | Enable debugging output |
| set recurse | Enable recursive queries |
| set norecurse | Disable recursion |
| set search | Use search list defined in /etc/resolv.conf |

**🔹 6. Reverse Lookups**

Query domain from IP:

nslookup 93.184.216.34

Query specific server:

nslookup 8.8.8.8 1.1.1.1

**🔹 7. Batch Mode**

Query multiple domains from file:

for d in $(cat domains.txt); do nslookup $d | grep Address; done

**🔹 8. Example Workflows**

**Workflow: Find Mail Servers**

nslookup -type=MX example.com

**Workflow: Get Nameservers**

nslookup -type=NS example.com

**Workflow: Check TXT/SPF Records**

nslookup -type=TXT example.com

**Workflow: Reverse IP → Domain**

nslookup 1.1.1.1

**🔹 9. nslookup vs dig vs host**

| **Tool** | **Features** |
| --- | --- |
| nslookup | Simple, available by default on most systems |
| dig | More powerful, detailed DNS info |
| host | Quick and simple queries |

**🔹 10. Tips & Notes**

* nslookup is deprecated in favor of dig, but still widely used.
* Always use -type for specific record lookups (faster & cleaner).
* For automation, combine with grep, awk, sed.
* Use **Google (8.8.8.8) / Cloudflare (1.1.1.1) / Quad9 (9.9.9.9)** for consistent queries.

⚡ With this cheat sheet, you can use nslookup for **A, MX, NS, TXT records, reverse lookups, debug mode, automation, and server-specific queries** like a pro.