**🌐 DNS Interrogation Techniques**

**(Part of OSINT & Reconnaissance)**

**🧠 What is DNS Interrogation?**

DNS (Domain Name System) acts like the **phonebook of the internet**.  
DNS interrogation means **digging deep into DNS records** to discover info about a target domain or network.

Used by **ethical hackers** to:

* Map domain infrastructure
* Find subdomains, IPs, MX (mail) records
* Spot misconfigurations
* Gather intelligence for later attacks

**🔧 Key DNS Interrogation Tools & Techniques**

| **Tool** | **Use** |
| --- | --- |
| nslookup | Get IP, mail server, DNS details |
| dig | Advanced DNS queries (more control, better info than nslookup) |
| Zone Transfer (AXFR) | Try to dump all DNS records from a misconfigured name server |
| Reverse DNS lookup | Get domain names from IPs |
| Subdomain brute-forcing | Find hidden subdomains |
| PTR Records | Map IPs to domains |
| host | Another simple DNS query tool |

**✅ Example Commands:**

* nslookup google.com → Basic DNS info
* dig google.com any → All records: A, MX, NS, etc.
* dig @nameserver.com target.com AXFR → Attempt zone transfer
* host -t mx gmail.com → Find mail servers

**🧪 Bonus Tools to Enhance DNS Interrogation**

| **Tool** | **What It Does** |
| --- | --- |
| **crt.sh / Cert Transparency** | Shows SSL certs for domains → helps find **related subdomains** |
| **Entrust.com CT** | Another cert transparency log viewer |
| **DNSDumpster** | Online DNS mapping & subdomain discovery |
| **Amass** | Automated subdomain enumeration |
| **HaveIBeenPwned.com** | Checks if domain/email was leaked or breached |
| **HackHoliday / NCSA** | Hacking CTF challenges that teach DNS, OSINT, and CTI skills |

**💡 DNS + OSINT Insights**

* **Cert Transparency Logs** are like a public log of all issued SSL certs.  
  Attackers use this to **discover new domains/subdomains** tied to a target.
* **Does OSINT data ever stop?**  
  ❌ **No.** OSINT is **always evolving.**  
  Every day new domains, emails, breaches, and logs appear.
* **DNS is a goldmine** because it’s usually **public**, and companies often forget to hide subdomains or close old ones.

**🧠 Why You Should Learn This:**

* It's **non-intrusive** (legal, passive scanning)
* Helps create a **full map of the target**
* Important for **red team recon** and **blue team defense**