Guide for Beginners DNS Footprinting Tool

By:Souleiman Guedi

Content

Introduction

What is DNS Footprinting?

DNS Footprinting is the process of collecting **DNS records, subdomains, IP addresses, and mail servers** associated with a target domain. It helps attackers (or ethical hackers) map out the target's infrastructure.

Why is it Important?

- Reveals **hidden subdomains** (e.g., admin.example.com).
- Identifies **misconfigured DNS servers** (e.g., open zone transfers).
- Helps in **phishing attacks** (finding email servers).
- Assists in **network mapping** (IP ranges, services).

Legal & Ethical Considerations

- **Only perform on authorized targets** (your own domain, bug bounty programs, or with permission).
- **Avoid aggressive scanning** (rate limits can block you).

Basic DNS Queries

Using `nslookup`

- Checks DNS records interactively.

set type=any

This tells nslookup to return any kind of DNS record it can find — like:

A (address) records

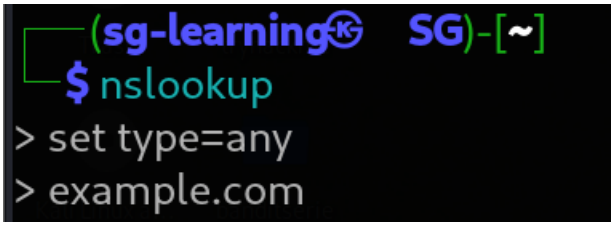
MX (mail) records

TXT (text) records

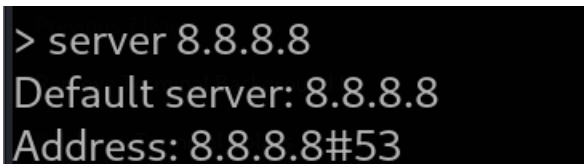
NS (name servers)

SOA (start of authority)

And more.



(**example.com**) This is the domain you're querying. It tells nslookup: "Give me all the DNS records you can find for example.com."If type=any is set, you'll get multiple types of records in one response.



- **Records to check:**
  - `A` (IPv4 address)
  - `AAAA` (IPv6 address)
  - `MX` (Mail servers)
  - `NS` (Nameservers)
  - `TXT` (SPF, DKIM, DMARC records)

Using `dig` (More Powerful)

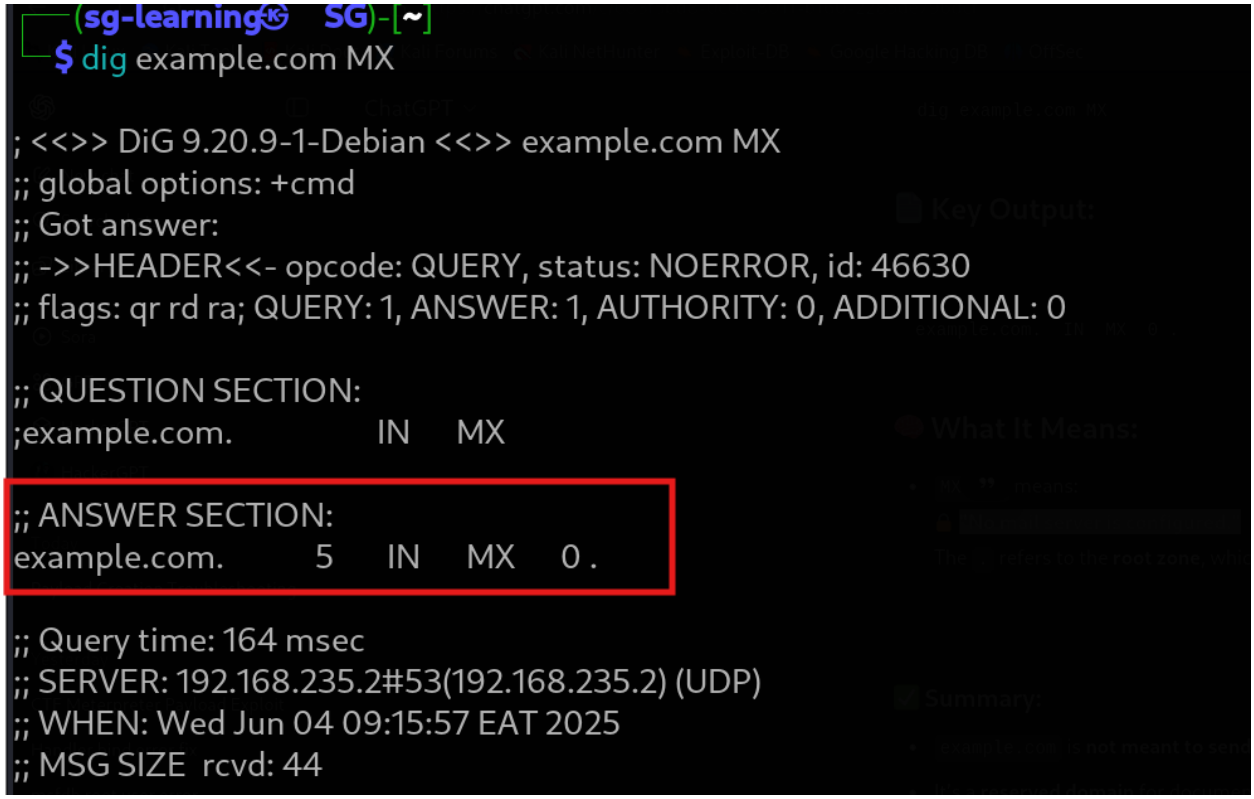
Dig example.com ANY @8.8.8.8 = All records

dig = DNS query tool

example.com = domain to query

ANY = request all DNS record types

@8.8.8.8 = use Google DNS server



MX 0. means: "No mail server is configured."

The. refers to the root zone, which effectively means no email is accepted for example.com.

Only IPs (faster)

```
┌──(sg-learning㉿SG)-[~]
└─$ dig example.com +short
96.7.128.175
96.7.128.198
23.192.228.80
23.192.228.84
23.215.0.136
23.215.0.138
```

Only IPs (faster) = **dig example.com +short**

- **Advanced uses:**
  - `+trace` → Follows DNS resolution path
  - `-x` → Reverse DNS lookup (IP → Domain)

```
┌──(sg-learning㉿SG)-[~]
└─$ dig example.com +trace

; <<>> DiG 9.20.9-1-Debian <<>> example.com +trace
;; global options: +cmd
.                       5       IN      NS      b.root-servers.net.
.                       5       IN      NS      d.root-servers.net.
.                       5       IN      NS      e.root-servers.net.
.                       5       IN      NS      h.root-servers.net.
.                       5       IN      NS      g.root-servers.net.
.                       5       IN      NS      j.root-servers.net.
.                       5       IN      NS      f.root-servers.net.
.                       5       IN      NS      a.root-servers.net.
.                       5       IN      NS      c.root-servers.net.
.                       5       IN      NS      m.root-servers.net.
.                       5       IN      NS      i.root-servers.net.
.                       5       IN      NS      l.root-servers.net.
.                       5       IN      NS      k.root-servers.net.
```

dig example.com +trace

This command performs a full DNS resolution trace, starting from the root DNS servers all the way down to the authoritative nameserver for example.com.

dig -x 8.8.8.8 only works with IP addresses, not domain names.

```
┌──(sg-learning㉿SG)-[~]
└─$ dig -x 8.8.8.8

; <<>> DiG 9.20.9-1-Debian <<>> -x 8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46692
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;8.8.8.8.in-addr.arpa.          IN      PTR

;; ANSWER SECTION:
8.8.8.8.in-addr.arpa.   5       IN      PTR     dns.google.

;; Query time: 8 msec
;; SERVER: 192.168.235.2#53(192.168.235.2) (UDP)
;; WHEN: Wed Jun 04 09:28:42 EAT 2025
;; MSG SIZE  rcvd: 62
```

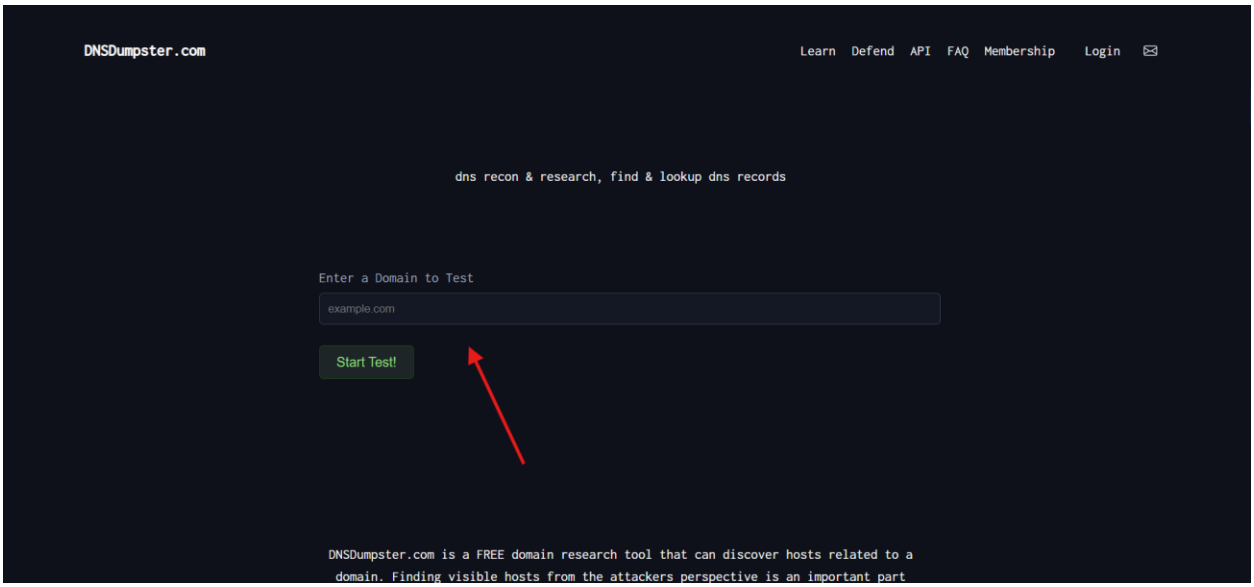
Subdomain Enumeration

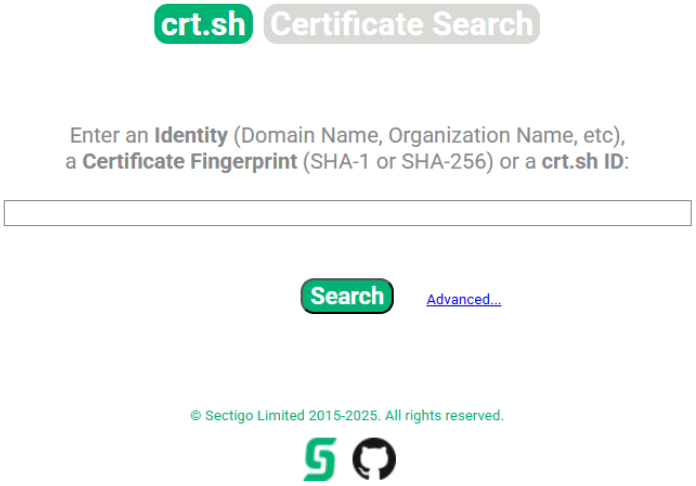
A. Passive Methods (No Direct Queries)

- **Tools:**
    - Sublist3r (scrapes Google, DNSdumpster, Netcraft)

```
┌──(sg-learning㉿SG)-[~]
└─$ sublist3r -d example.com -o subdomains.txt
```

- **Online Tools:**
    - DNSdumpster
    - Crt.sh (Finds subdomains via SSL certificates)





B. Active Methods (Brute-Forcing)

- **Wordlist-based attacks:**

```
(sg-learning㉿SG)-[~]
$ gobuster dns -d example.com -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-5000.txt -t threads 50
```

Uses wordlists (/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top-5000.txt)

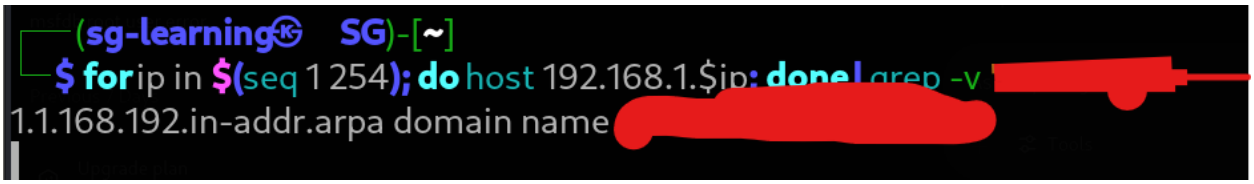
DNS Zone Transfers (AXFR)

What is a Zone Transfer?

- A DNS server **sends all records** to another server (misconfigured if public).
- **Exploitable if allowed:**

Reverse DNS Lookup

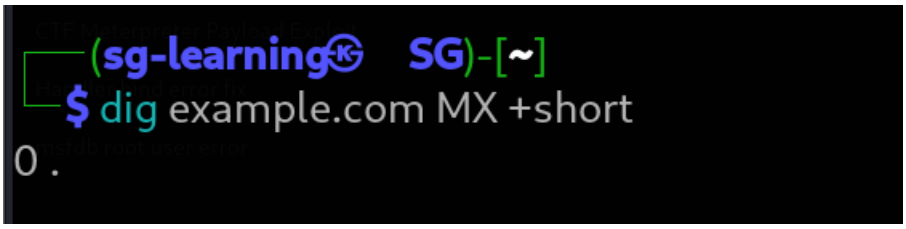
- Finds **domains linked to an IP range**.



- Useful for **finding hidden services**.

Mail Server Enumeration

- **Find MX records:**



- **Check for misconfigurations:**
  - Open relays
  - Weak SPF/DKIM/DMARC policies

DNS Brute-Forcing (Advanced)

- **Using** `dnsenum`**:**

- Combines **Google scraping, brute-forcing, and zone transfer checks**.

dnsenum = DNS enumeration tool to gather info about domains.

example.com = target domain.

--threads 10 = run with 10 concurrent threads (faster scanning).

-o report.xml = save the output/results in XML format to report.xml.

Reporting & Documentation

- **Structure your findings:**

```
# DNS Footprinting Report - example.com

## Subdomains Found
- admin.example.com
- dev.example.com

## Vulnerabilities
- Open AXFR on ns1.example.com
```

- **Tools for automation:**

- `Metasploit` (`auxiliary/gather/dns_info`)
- `DNSRecon` (XML/CSV reports)

Bonus: Automation & Scripting

Bash Script Example

```
#!/bin/bash
domain=$1
echo "[+] Running DNS recon on $domain"
dig $domain ANY +noall +answer
dnsrecon -d $domain -t std,axfr -j report.json
```

- **Scheduled monitoring:**
  - Use cron to run weekly scans.

Legal & Best Practices

- **Always get permission** before scanning.
- **Use rate-limiting** to avoid detection.
- **Avoid illegal activities** (unauthorized hacking is a crime).

Helpful Artifacts

Cheat Sheet

```
1. `dig example.com ANY` → All records
2. `dnsrecon -d example.com` → Subdomains
3. Check AXFR: `dig @ns1 example.com AXFR`
```

Checklist

- ☑ Basic DNS queries (`nslookup`, `dig`)
- ☑ Subdomain enumeration (`Sublist3r`, `dnsenum`)
- ☑ Mail server checks (`MX`, `TXT`)
- ☑ Report findings