

Digging DNS

Having established a solid understanding of DNS fundamentals and its various record types, let's now transition to the practical. This section will explore the tools and techniques for leveraging DNS for web reconnaissance.

DNS Tools

DNS reconnaissance involves utilizing specialized tools designed to query DNS servers and extract valuable information. Here are some of the most popular and versatile tools in the arsenal of web recon professionals:

Tool	Key Features	Use Cases
dig	Versatile DNS lookup tool that supports various query types (A, MX, NS, TXT, etc.) and detailed output.	Manual DNS queries, zone transfers (if allowed), troubleshooting DNS issues, and in-depth analysis of DNS records.
nslookup	Simpler DNS lookup tool, primarily for A, AAAA, and MX records.	Basic DNS queries, quick checks of domain resolution and mail server records.
host	Streamlined DNS lookup tool with concise output.	Quick checks of A, AAAA, and MX records.
dnsenum	Automated DNS enumeration tool, dictionary attacks, brute-forcing, zone transfers (if allowed).	Discovering subdomains and gathering DNS information efficiently.
fierce	DNS reconnaissance and subdomain enumeration tool with recursive search and wildcard detection.	User-friendly interface for DNS reconnaissance, identifying subdomains and potential targets.
dnsrecon	Combines multiple DNS reconnaissance techniques and supports various output formats.	Comprehensive DNS enumeration, identifying subdomains, and gathering DNS records for further analysis.
theHarvester	OSINT tool that gathers information from various sources, including DNS records (email addresses).	Collecting email addresses, employee information, and other data associated with a domain from multiple sources.
Online DNS Lookup Services	User-friendly interfaces for performing DNS lookups.	Quick and easy DNS lookups, convenient when command-line tools are not available, checking for domain availability or basic information

The Domain Information Groper

The **dig** command (**Domain Information Groper**) is a versatile and powerful utility for querying DNS servers and retrieving various types of DNS records. Its flexibility and detailed and customizable output make it a go-to choice.

Common dig Commands

Command	Description
dig domain.com	Performs a default A record lookup for the domain.
dig domain.com A	Retrieves the IPv4 address (A record) associated with the domain.
dig domain.com AAAA	Retrieves the IPv6 address (AAAA record) associated with the domain.
dig domain.com MX	Finds the mail servers (MX records) responsible for the domain.
dig domain.com NS	Identifies the authoritative name servers for the domain.
dig domain.com TXT	Retrieves any TXT records associated with the domain.
dig domain.com CNAME	Retrieves the canonical name (CNAME) record for the domain.
dig domain.com SOA	Retrieves the start of authority (SOA) record for the domain.
dig @1.1.1.1 domain.com	Specifies a specific name server to query; in this case 1.1.1.1
dig +trace domain.com	Shows the full path of DNS resolution.
dig -x 192.168.1.1	Performs a reverse lookup on the IP address 192.168.1.1 to find the associated host name. You may need to specify a name server.
dig +short domain.com	Provides a short, concise answer to the query.
dig +noall +answer domain.com	Displays only the answer section of the query output.
dig domain.com ANY	Retrieves all available DNS records for the domain (Note: Many DNS servers ignore ANY queries to reduce load and prevent abuse, as per RFC 8482).

Caution: Some servers can detect and block excessive DNS queries. Use caution and respect rate limits. Always obtain permission before performing extensive DNS reconnaissance on a target.

Groping DNS

```

MisaelMacias@htb[/htb]$ dig google.com

; <>> Dig 9.18.24-0ubuntu0.22.04.1-Ubuntu <>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 16449
;; Flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 0       IN      A      142.251.47.142
```

[📄 Cheat Sheet](#)[? Go to Questions](#)

Table of Contents

Introduction

[Introduction](#) ✓

WHOIS

[WHOIS](#) ✓[🔗 Utilizing WHOIS](#) ✓

DNS & Subdomains

[DNS](#) ✓[🔗 Digging DNS](#) ✓[Subdomains](#) ✓[🔗 Subdomain Bruteforcing](#) ✓[🔗 DNS Zone Transfers](#) ✓[🔗 Virtual Hosts](#) ✓[Certificate Transparency Logs](#) ✓

Fingerprinting

[🔗 Fingerprinting](#) ✓

Crawling

[Crawling](#) ✓[robots.txt](#) ✓[.Well-Known URIs](#) ✓[🔗 Creepy Crawlies](#) ✓

Search Engine Discovery

[Search Engine Discovery](#) ✓

Web Archives

[🔗 Web Archives](#) ✓

Automating Recon

[Automating Recon](#) ✓

Skills Assessment

[🔗 Skills Assessment](#) ✓

My Workstation

OFFLINE

[🔗 Start Instance](#)

∞ / 1 spawns left

```
;; Query time: 0 msec
;; SERVER: 172.23.176.1#53(172.23.176.1) (UDP)
;; WHEN: Thu Jun 13 10:45:58 SAST 2024
;; MSG SIZE rcvd: 54
```

This output is the result of a DNS query using the `dig` command for the domain `google.com`. The command was executed on a system running `Dig` version `9.18.24-0ubuntu0.22.04.1-Ubuntu`. The output can be broken down into four key sections:

1. Header

- `;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16449`: This line indicates the type of query (`QUERY`), the successful status (`NOERROR`), and a unique identifier (`16449`) for this specific query.
- `;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0`: This describes the flags in the DNS header:
 - `qr`: Query Response flag - indicates this is a response.
 - `rd`: Recursion Desired flag - means recursion was requested.
 - `ad`: Authentic Data flag - means the resolver considers the data authentic.
 - The remaining numbers indicate the number of entries in each section of the DNS response: 1 question, 1 answer, 0 authority records, and 0 additional records.
- `;; WARNING: recursion requested but not available`: This indicates that recursion was requested, but the server does not support it.

2. Question Section

- `;google.com. IN A`: This line specifies the question: "What is the IPv4 address (A record) for `google.com`?"

3. Answer Section

- `google.com. 0 IN A 142.251.47.142`: This is the answer to the query. It indicates that the IP address associated with `google.com` is `142.251.47.142`. The '0' represents the `TTL` (time-to-live), indicating how long the result can be cached before being refreshed.

4. Footer

- `;; Query time: 0 msec`: This shows the time it took for the query to be processed and the response to be received (0 milliseconds).
- `;; SERVER: 172.23.176.1#53(172.23.176.1) (UDP)`: This identifies the DNS server that provided the answer and the protocol used (UDP).
- `;; WHEN: Thu Jun 13 10:45:58 SAST 2024`: This is the timestamp of when the query was made.
- `;; MSG SIZE rcvd: 54`: This indicates the size of the DNS message received (54 bytes).


An `opt_pseudosection` can sometimes exist in a `dig` query. This is due to Extension Mechanisms for DNS (`EDNS`), which allows for additional features such as larger message sizes and DNS Security Extensions (`DNSSec`) support.

If you just want the answer to the question, without any of the other information, you can query `dig` using `+short`:

Digging DNS

```
MisaelMacias@ntb[/ntb]$ dig +short hackthebox.com

104.18.20.126
104.18.21.126
```



Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK19ms

Terminate Pwnbox to switch location

Start Instance

00 / 1 spawns left

Waiting to start...

Questions

Answer the question(s) below to complete this Section and earn cubes!



Cheat Sheet

+ 1 🟢 Which IP address maps to inlanefreight.com?

134.209.24.248

Submit

+ 1 🟢 Which domain is returned when querying the PTR record for 134.209.24.248?

cloudmonitor30.paypal.com

Submit

+ 0 🟢 What is the full domain returned when you query the mail records for facebook.com?

mx1.paypalcorp.com

Submit

← Previous Next →

Mark Complete & Next

