DigDug

> **Instructions**
> Oooh, turns out, this `10.10.198.23` machine is also a DNS server! If we could `dig` into it, I am sure we could find some interesting records! But... it seems weird, this only responds to a special type of request for a `givemetheflag.com` domain?

Review Knowledge

Definitions

DNS (Domain Name System) provides a simple way for us to communicate with devices on the internet without remembering complex numbers

Record Types

Query type	Result
A	IPv4 Addresses
AAAA	IPv6 Addresses
CNAME	Canonical Name
MX	Mail Servers
SOA	Start of Authority
TXT	TXT Records

Reconnaissance Tools

- nslookup
- dig

Walkthrough

First of all, take a look at the **Instructions** one more time. There are 3 given hints:

- DNS server: `10.10.198.23`
- Tool to use: `dig`
- Domain: `givemetheflag.com`

`Dig` Usage:

```
dig @[global-server] [domain] [record-type]
```

Let's try using `dig` with a normal public `global-server` and `domain` at first to view the result:

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ dig @8.8.8.8 tryhackme.com

; <<>> DiG 9.18.12-1-Debian <<>> @8.8.8.8 tryhackme.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52019
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;tryhackme.com.                 IN      A

;; ANSWER SECTION:
tryhackme.com.          300     IN      A       104.22.55.228
tryhackme.com.          300     IN      A       104.22.54.228
tryhackme.com.          300     IN      A       172.67.27.10

;; Query time: 32 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Jul 30 09:04:11 EDT 2023
;; MSG SIZE  rcvd: 90
```

Or embed the `record-type`:

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ dig @8.8.8.8 tryhackme.com TXT

; <<>> DiG 9.18.12-1-Debian <<>> @8.8.8.8 tryhackme.com TXT
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4123
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;tryhackme.com.                 IN      TXT

;; ANSWER SECTION:
tryhackme.com.          300     IN      TXT     "google-site-verification=umR4x8HuzWMF5g36
56JY1b-61NuryD0-GqGnYN13ONo"
tryhackme.com.          300     IN      TXT     "v=spf1 include:_spf.google.com include:em
ail.chargebee.com ~all"

;; Query time: 51 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Sun Jul 30 09:05:42 EDT 2023
;; MSG SIZE  rcvd: 199
```

Enumerate the target

```
┌──(kali㉿kali)-[~/TryHackMe]
└─$ dig @10.10.198.23 givemetheflag.com

; <<>> DiG 9.18.12-1-Debian <<>> @10.10.198.23 givemetheflag.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43399
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
givemetheflag.com.      0       IN      TXT     "flag{0767ccd06e79853318f25aeb08ff83e2}"
```

```
;; Query time: 187 msec
;; SERVER: 10.10.198.23#53(10.10.198.23) (UDP)
;; WHEN: Sun Jul 30 09:09:09 EDT 2023
;; MSG SIZE  rcvd: 86
```

We got the flag at the first try!