Exercise 1d: Working with Command Line Tools – dig

Date: 02.03.2023

Prerequisites

- A system running Linux
- A user account with sudo or root privileges
- Access to a terminal window / command line

What is dig?

DIG command (Domain Information Groper command) is a network tool with a basic command-line interface that serves for making different DNS (domain name system) queries. You can use the DIG command to:

- Diagnose your name servers. Check all of them or each individual server and their response.
- Check all of the available DNS records or individual DNS records and their parameters.
- Trace IP addresses and see the hostnames that correspond to them.
- Do a query through a specific port that you want to use.
- See the TTL value of the DNS records and know, how often, do they refresh.
- Trace the route of a DNS query.

Install dig on Linux (Optional)

Most modern Linux systems include the **dig** command.

Verify that it's installed by checking the software version. To do so, open a command line and enter the following:

```
dig -v
```

The system should respond with a numeric code. If the system can't find the command specified, install dig by entering the following:

Debian / Ubuntu:

```
sudo apt-get install dnsutils
```

dig Syntax

The **dig** command is used as follows:

```
dig [server] [name] [type]
```

[server] – The hostname or IP address the query is directed to
[name] – The DNS (Domain Name Server) of the server to query
[type] – The type of DNS record to retrieve. By default (or if left blank), **dig** uses the A record type

How to Use the dig Command With Examples

Let's look at the basic usage of the **dig** command.

DNS Lookup

The **dig** command enables searching for a domain name. To perform a DNS lookup, open the terminal and type:

```
dig google.com
```

The most important section is the **ANSWER** section:

- The first column lists the name of the server that was queried
- The second column is the **Time to Live**, a set timeframe after which the record is refreshed
- The third column shows the class of query – in this case, "IN" stands for Internet
- The fourth column displays the type of query – in this case, "A" stands for an A (address) record
- The final column displays the IP address associated with the domain name

Note:

- A record refers to IPV4 IP.
  Similarly, if record type is set as "AAAA", this would return IPV6 IP.

Other lines can be translated as follows:

- The **first line** displays the version of the **dig** command.
- The **HEADER** section shows the information it received from the server. Flags refer to the answer format.

The **OPT PSEUDOSECTION** displays advanced data:

- EDNS – Extension system for DNS, if used
- Flags – blank because no flags were specified
- UDP – UDP packet size

The **QUESTION** section displays the query data that was sent:

- First column is the domain name queried
- Second column is the type (IN = Internet) of query
- Third column specifies the record (A = Address), unless otherwise specified

The **STATISTICS** section shows metadata about the query:

- Query time – The amount of time it took for a response
- SERVER – The IP address and port of the responding DNS server. You may notice a loopback address in this line – this refers to a local setting that translates DNS addresses
- WHEN – Timestamp when the command was run
- MSG SIZE rcvd – The size of the reply from the DNS server

ANY Option

To return all of the results of the query, use the following:

```
dig google.com ANY
```

The system will list all **google.com** DNS records that it finds, along with the IP addresses.

Short Answer Option

To display only the IP address associated with the domain name, enter the following:

```
dig google.com +short
```

Detailed Answer Option

Run **+noall +answer** with the **dig** command to access detailed information in the *answers* section:

```
dig google.com +noall +answer
```

Trace Option

The **+trace** option lists each different server the query goes through to its final destination. Use this command option to identify the IP address where traffic is dropping.

```
Dig google.com +trace
```

Reverse DNS Lookup

To look up a domain name by its IP address, type the following:

```
dig -x 172.217.14.238
```

The **-x** option allows you to specify the IP address instead of a domain name. This can be combined with other options:

```
dig +noall +answer -x 172.217.14.238
```

How to find the website's IP address?

Find the IP address of a particular domain name that you want to know. You can use the dig command, without any additional option, which is:

dig google.com
It will do a DNS query, looking for the A records. They have the IP addresses which correspond to the domain name form the query.

*****