Practical work 3 - Secure DNS and web servers

Security

Sébastien Vaucher
sebastien.vaucher@unine.ch

27 October 2021

In this practical work, you are going to install and configure a Linux server following current best practices regarding security. You will start by hosting a DNS zone, that will then serve to point to an HTTPS server. The DNS zone will be signed using Domain Name System Security Extensions (DNSSEC)[1].

Please read this document in full at least once before starting.

1 Serving a signed DNS zone

In this first part, you will be given the responsibility of managing a DNS zone under the `sec21.tech` domain. The domain label has either been chosen by yourself, *i.e.*, you have notified the TA before, or it has been assigned for you by the TA.

The first task is to choose which authoritative DNS server you want to use. I strongly recommend Knot DNS[2] as it supports automatic DNSSEC signing, and is easy to configure. As always, you are free to choose a different piece of software.

[1] https://www.cloudflare.com/dns/dnssec/how-dnssec-works/
[2] https://www.knot-dns.cz/

1.1 Basic zone

We start with the simplest DNS zone file possible, containing information regarding your sub-domain and the necessary *glue* to have a functional zone.

The TA has already added an `NS` (nameserver)[3] record in the parent zone `sec21.tech` to delegate control of your sub-domain (hereafter referred to as `yourdomain.sec21.tech`) to your machine. A *glue record* on `ns.yourdomain.sec21.tech` pointing towards your machine has also been configured.

Here is a summary of your tasks for this part.

1. Install the chosen authoritative DNS server (the instructions assume that you chose Knot DNS).
   - *Note:* the version of Knot DNS that is available in the official package repositories from Ubuntu is outdated. The people behind Knot DNS provide a Personal Package Archive (PPA) containing up-to-date packages[4].
2. Configure the server to listen on port 53 on its private IP address (`172.28.x.x`).
3. We start with the simplest DNS zone file possible, containing information regarding your sub-domain and the necessary *glue* to have a functional zone. Please give the name `ns` to your name server. In our case, we only have one name server, but in practice having `2` or mode is strongly recommended for redundancy.

   Your zone should look like the following (replace `yourdomain` with your sub-domain name, and adapt other values where necessary).

   ```
   yourdomain.sec21.tech.      3600  SOA  ns.yourdomain.sec21.tech.
   ↪  hostmaster.invalid. 2021102700 600 600 604800 60
   yourdomain.sec21.tech.      3600  NS   ns.yourdomain.sec21.tech.
   ns.yourdomain.sec21.tech.  3600  A    192.42.43.4x
   ```

4. Save your zone file, and register it for your domain in the configuration file of the server.
5. Reload your server to take your changes into account (`knotc reload` for Knot DNS).
6. Check the logs of your server for any errors (`journalctl -xeu knot` for Knot DNS).
7. Check whether your domain can be successfully resolved. You can use an online service to thoroughly check your work[5]. There should not be any warnings or errors except for DNSSEC-related warnings which are expected and will be removed in the next steps. If there are other warnings and/or errors, you must fix them before continuing.
   Do not hesitate to ask for help if you feel stuck!

[3] http://www.zytrax.com/books/dns/ch8/ns.html
[4] https://launchpad.net/~cz.nic-labs/+archive/ubuntu/knot-dns-latest
[5] *E.g.*, https://dnscheck.norid.no/en or https://dnsviz.net/

1.2 Signing the zone with DNSSEC

In this step, you will cryptographically sign your zone with DNSSEC, in a way that allows anyone to check its authenticity.

Here is a summary of the tasks involved to sign the zone.

1. Enable automatic DNSSEC signing, or follow the official documentation of your DNS server to manually sign the zone.

   a) In Knot DNS, enabling automatic signing is as simple as setting `dnssec-signing`: `on` in its configuration file, *i.e.*,

   ```
   zone:
    - domain: yourdomain.sec21.tech
      dnssec-signing: on
   ```

   Knot handles all the heavy lifting of generating public/private key-pairs and then signing the zone. It also automatically handles key rollovers. You can customize the behavior of Knot by specifying the `dnssec-policy`[6] key.

2. Reload your server (`knotc reload`).

3. Push the DS (delegation signer) record(s) to the `sec21.tech` zone, which will extend the chain of trust from `sec21.tech` to your chosen sub-domain.

   a) Knot DNS can automatically push the record(s) using Dynamic DNS (DDNS) by setting the `ds-push`[7] and `ksk-submission`[8] directives, pointing to the hidden primary DNS server of `sec21.tech`: `20.93.158.230`.

   b) If you really struggle with the automatic way, you can communicate the DS record(s) to the TA who will manually add them to the `sec21.tech` zone. Here is the information that you need to communicate:

   Key tag the identifier of the key, which is a number between 0 and 65535.

   Algorithm type each allowed algorithm in DNSSEC has a specified number[9]. *E.g.*, algorithm 13 is ECDSA with a P-256 curve using SHA-256.

   Digest type the hash function used to generate the digest from the public key [10].

   The digest itself A long string, *i.e.*, the hash of the public key.

   Knot DNS will give all the information you need with the command

   ```
   # keymgr yoursubdomain.sec21.tech ds
   ```

   Organizational concern: you can skip ahead to section 2 while you wait for the TA to install the DS record.

4. Check[3] whether your zone can be successfully authenticated.

[6] https://www.knot-dns.cz/docs/3.1/html/reference.html#policy-section
[7] https://www.knot-dns.cz/docs/3.1/html/reference.html#ds-push
[8] https://www.knot-dns.cz/docs/3.1/html/reference.html#ksk-submission
[9] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml
[10] https://www.iana.org/assignments/ds-rr-types/ds-rr-types.xhtml

Delegation Signer records

`DS` records are hashes of the public key linked to the zone. They are in place for every level of the DNS tree up to the root, which is what allows anyone to check the *authenticity* of any zone signed with DNSSEC. The `DS` record of the root key-signing key (KSK)[a] is manually installed on every resolver to bootstrap the chain.

[a] `https://data.iana.org/root-anchors/root-anchors.xml`

2 Secure web server

So far, you have configured a perfectly functional domain, but it is empty. As a domain without anything in it is boring and mostly useless, you will configure what is probably the most common service on the Internet: a web server. As this is a lecture focused on security, you will install and configure your web server following the current best security practices.

Your server can serve any website; it can be as simple as a single web page.

2.1 Adding an `A` record for `www`

Before starting, you need to create a record of type `A` (IPv4 address) called `www` in your zone. It will contain the public IP address of your machine as value. Choose a small value for the TTL field (60 seconds is fine; that is the time you will have to wait if you make a mistake).

Perform the necessary steps to commit your change.

Do not configure an `A` record on the apex of your domain!

2.2 Installing and configuring the web server

Your task is to install and configure a web server that complies with the following criteria.

1. Has a good track record regarding security
2. Supports HTTPS connections
   a) Your server must present a certificate that is trusted by most modern browsers, *e.g.*, signed by the *Let's Encrypt* free certificate authority[11].
   b) If you are using *Let's Encrypt*, please note that there is a rate limitation on certificates generation[12].

[11] `https://letsencrypt.org/`
[12] `https://letsencrypt.org/docs/rate-limits/`

c) For this assignment, the certificate must be valid for `www.yourdomain.sec21.tech`.

In a future assignment, you will need to cover additional domains, so it can be worthwhile to spend some time now to obtain a wildcard certificate valid for `yourdomain.sec21.tech` *and* `*.yourdomain.sec21.tech`*.*

3. Configured with either the *Intermediate* or *Modern* configuration recommended by Mozilla[13]
4. Plaintext HTTP requests will be redirected to the equivalent HTTPS URL
5. The HTTP Strict Transport Security (HSTS) header will be served

You can use any web server for this task. NGINX or the Apache HTTP server are recommended for proficient users. Beginners can try Caddy instead[14]. You can use the *testssl.sh*[15] utility, as well as the *Security Headers*[16] website to help you judge the security of your configuration. Note that the grades given by these tools only give an estimation, not a proof of the security offered by your server.

2.3 Hand-in

The time allotted for this assignment is 2 weeks. The deadline is on 10 November at 14:15.

You will write a succinct report that explains your choices, the problems you might have encountered, and the steps you took to test your work. You will attach a commented log of all the commands that you executed on your server in an appendix of your report. Reading that report should allow you to replicate your work in the future.

You will also make a backup of your DNS zone file and any configuration file that you modify.

Should you implement relevant additions (see section 3), you will document them in your report, briefly explaining how security is improved thanks to them.

- To be submitted to Ilias:
  - Report as described above, in PDF, Markdown, or raw text format
  - Backup of all configuration files that you modified
  - All the files have to be packed in an archive in a standard format, named following this exact pattern, in lowercase letters only:
    `security21_as3_<your family names>.<extension>`
    For example, if your names were to be *Homer J. Simpson* and *Philip J. Fry*, you would use the following filename for this assignment:
    `security21_as3_simpson_fry.tar.gz`
  - Please use the "Upload File" button when handing-in your assignment in Ilias. Do **not** use "Upload Multiple Files as Zip-Archive".

[13] https://ssl-config.mozilla.org/
[14] https://caddyserver.com/docs
[15] https://github.com/drwetter/testssl.sh
[16] https://securityheaders.com/

- You must demonstrate your solution to the assistant during the exercise session, at the latest during the week that follows the deadline. It is **mandatory** for each team to demonstrate their submission!

3 Grading

These criteria will be taken into account to grade your work.

- Functionality of the DNS server
  - The DNS server replies to requests with valid content
  - The DNS zone has the right contents
  - DNSSEC is correctly configured
  - `www.yourdomain.sec21.tech` points to your web server
  - `yourdomain.sec21.tech` **does not** point to your web server
- Functionality of the web server
  - The web server replies to requests with some content
  - HTTPS is available with a valid certificate
  - HTTP requests are redirected to an equivalent HTTPS URL
  - HSTS is enabled with a long enough `max-age`
  - Mozilla's configuration recommendations are followed
- Hand-in according to the instructions above
- General quality of your report
- In-class demonstration

You are encouraged to implement relevant security-related additions, which might add bonus points to your grade, at the TA's discretion.