CS 432/532 – Computer and Network Security – Spring 2025

Lab #3

Creating a web server certificate for SSL and SSL configuration

Installation Steps

1. You can skip that step if you are using Kali Linux image since it already has nginx installed. Otherwise do the following:
   - ○ Install nginx web server using apt-get package manager (See section "Commands" below).
2. Decide on your own domain name. You can use "*yourSUid.lab*" as your domain name (e.g batuhankertmen.*lab*). Edit your host file (located in /etc/hosts) in order to resolve this domain to local IP address.

Certificate Generation Steps

3. Create 4096 bit RSA key pair for CA (Certification Authority) key file (for example ca.key)
4. Create CA certificate file (for example ca.crt) valid for 365 days.
5. Create 4096 bit RSA Web Server key pair (for example server.key)
6. Create Certificate Sign Request file (for example server.csr) for the web server certificate.
7. Sign web server certificate request (the csr file) file using previously created CA certificate. This process yields web server certificate file (for example server.crt).
8. The above steps create a shielded (i.e. encrypted) private key. You have to use raw private key in SSL. So you have un-shield it (required for Nginx).

For the required commands for these steps, please see "Commands" section.

Web Server Configuration Steps

9. Edit default server configuration for the SSL requests.
10. Start nginx web server.

Test Steps

11. Import CA certificate to Firefox web browser.

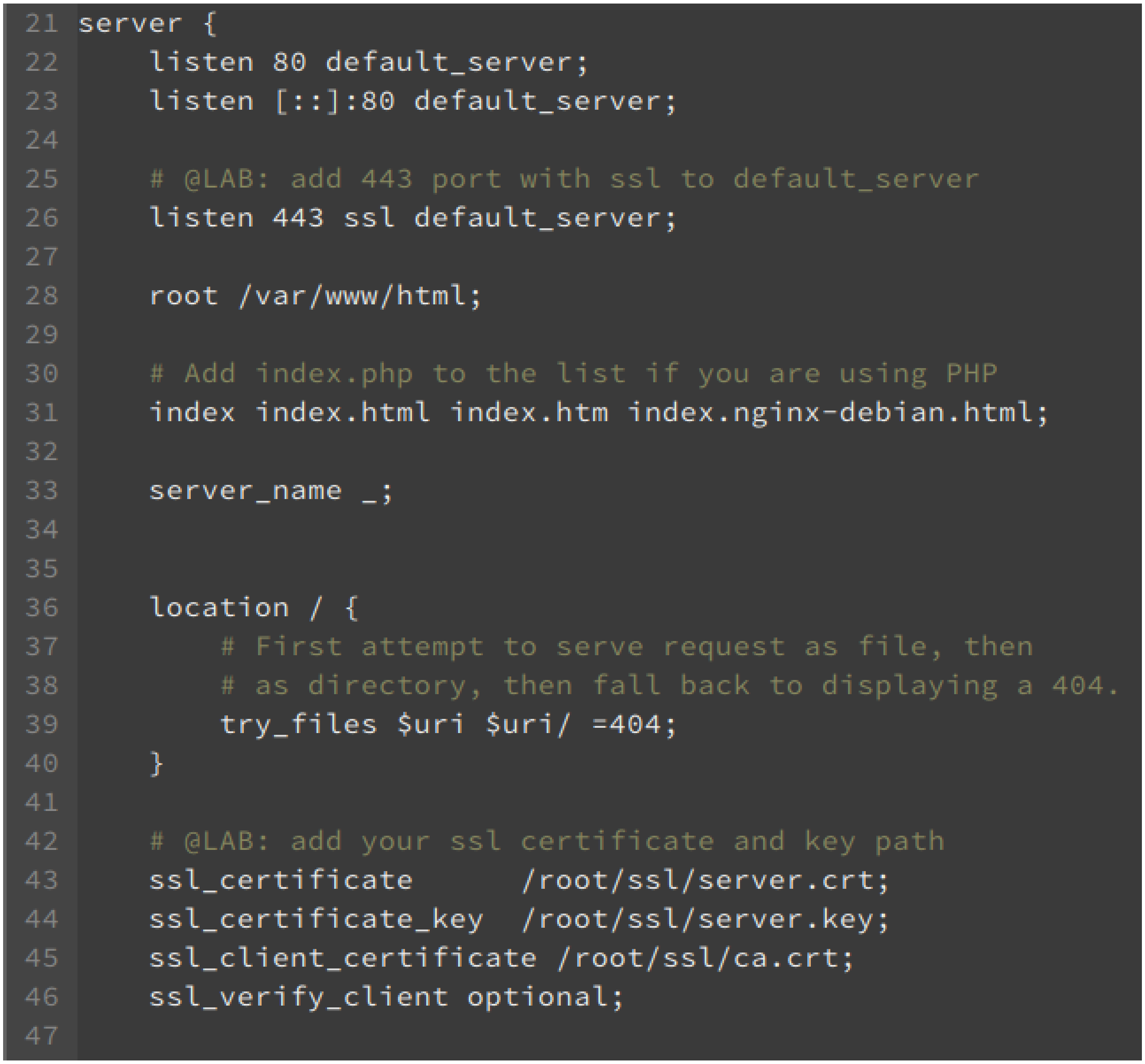
12. Browse *“https://yourSUid.lab”* domain.

Commands

- Install package: apt-get install <package_name>
  - apt-get install nginx
- Service management: systemctl <command> <service>
  - systemctl start nginx
  - systemctl restart nginx
  - systemctl stop nginx
  - systemctl status nginx
- Creating a *key* file: openssl genrsa -<algo> -out <keyfile> <bitsize>
  - Example: openssl genrsa -out my.key 2048
- Creating CA certificate file:
  openssl req -new -x509 -days <valid_days> -key <keyfile> -out <crtfile>
  - Example: openssl req -new -x509 -days 100 -key ca.key -out ca.crt
- Creating CSR file: openssl req -new -key <keyfile> -out <csrfile>
  - Example: openssl req -new -key server.key -out server.csr
- Signing certificate request: openssl x509 -req -extfile <(printf "subjectAltName=DNS: *yourSUid.lab* ") -days <valid_days> -in <csrfile> -CA <cacrt> -CAkey <cakey> -set_serial <serialNumber> -out <servercrt>
  - Example: openssl x509 -req -extfile <(printf "subjectAltName=DNS:batuhankertmen.lab ") -days 100 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt
- Un-shielding web server private key (required for Nginx).
  - cp server.key server.key.tmp
  - openssl rsa -in server.key.tmp -out server.key
- For controlling the contents of the certificates
  - openssl x509 -in <crtfile> -text -noout
  - openssl req -noout -text -in <csrfile>

Web Server Configuration

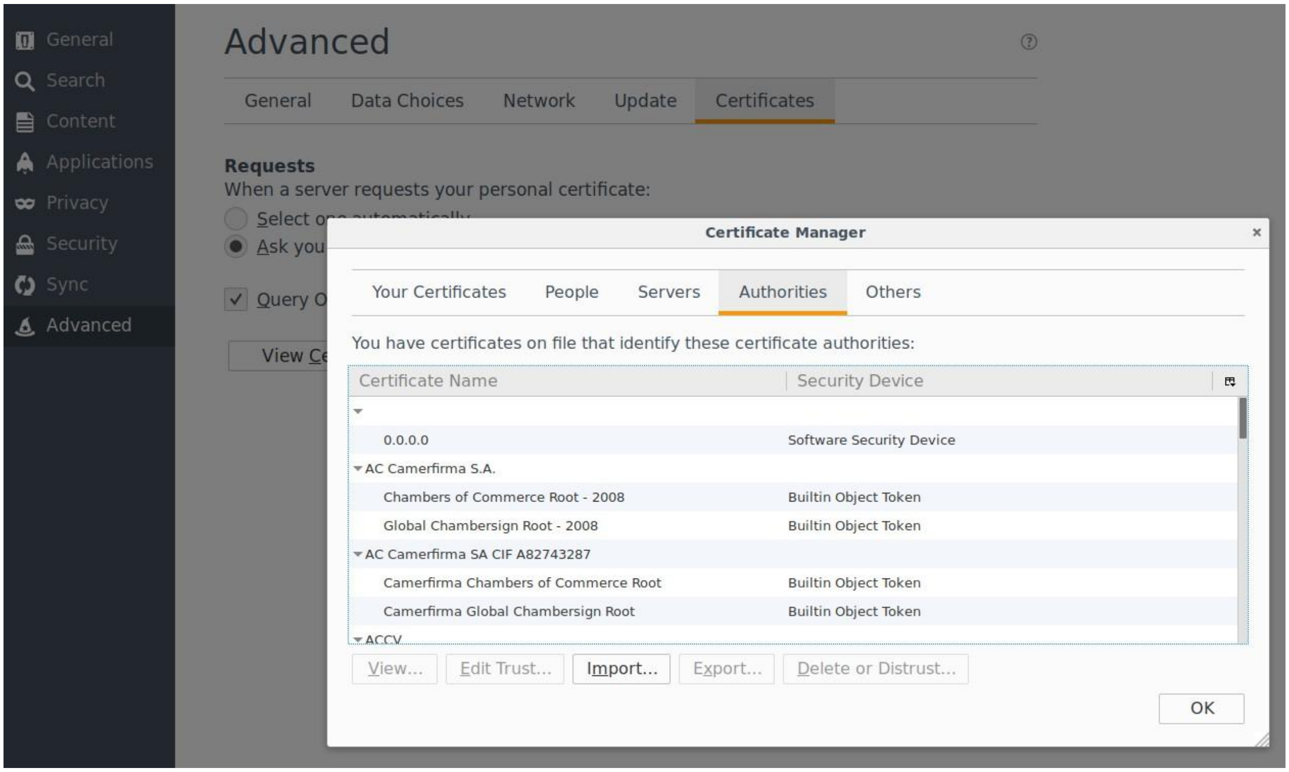
- Add lines beginning with the “@LAB” to “/etc/nginx/sites-enabled/default” file. Do not forget to change certificate and key paths.



```
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # @LAB: add 443 port with ssl to default_server
    listen 443 ssl default_server;

    root /var/www/html;

    # Add index.php to the list if you are using PHP
    index index.html index.htm index.nginx-debian.html;

    server_name _;


    location / {
        # First attempt to serve request as file, then
        # as directory, then fall back to displaying a 404.
        try_files $uri $uri/ =404;
    }

    # @LAB: add your ssl certificate and key path
    ssl_certificate       /root/ssl/server.crt;
    ssl_certificate_key   /root/ssl/server.key;
    ssl_client_certificate /root/ssl/ca.crt;
    ssl_verify_client optional;

```

Import CA Certificate to Browser

- First, open settings tab.
- Search for “certificate” in the search bar and click “View Certificates”.
- Import “ca.crt” file to “Authorities”.

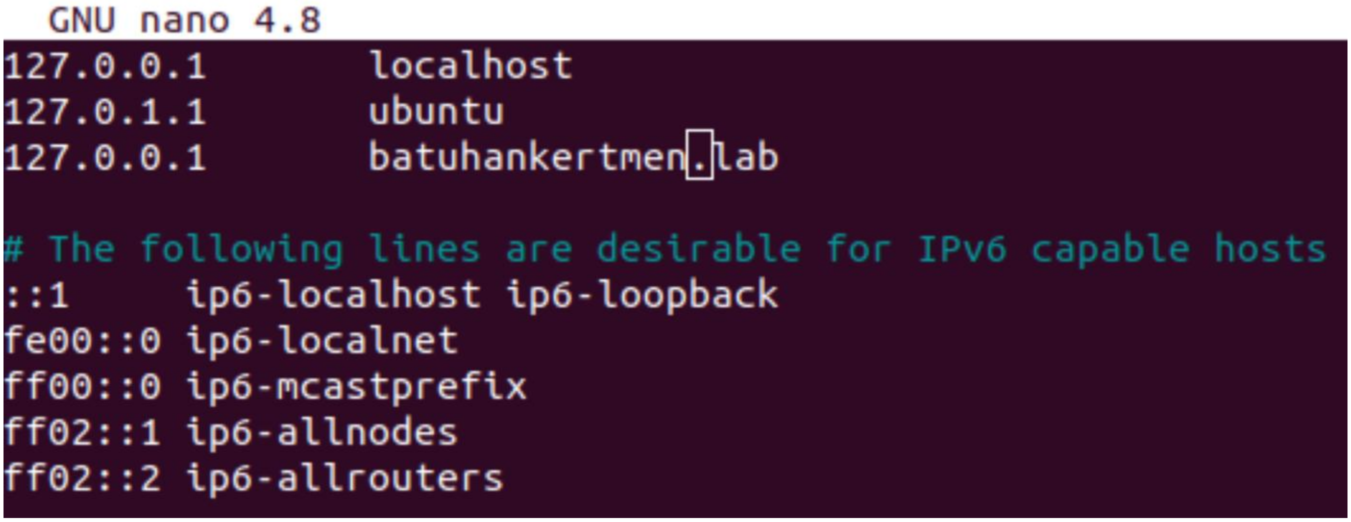


You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device
▾	
0.0.0.0	Software Security Device
▾ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
▾ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
▾ ACCV	

Host File Configuration

- Add new line to “/etc/hosts” file for the custom domain.



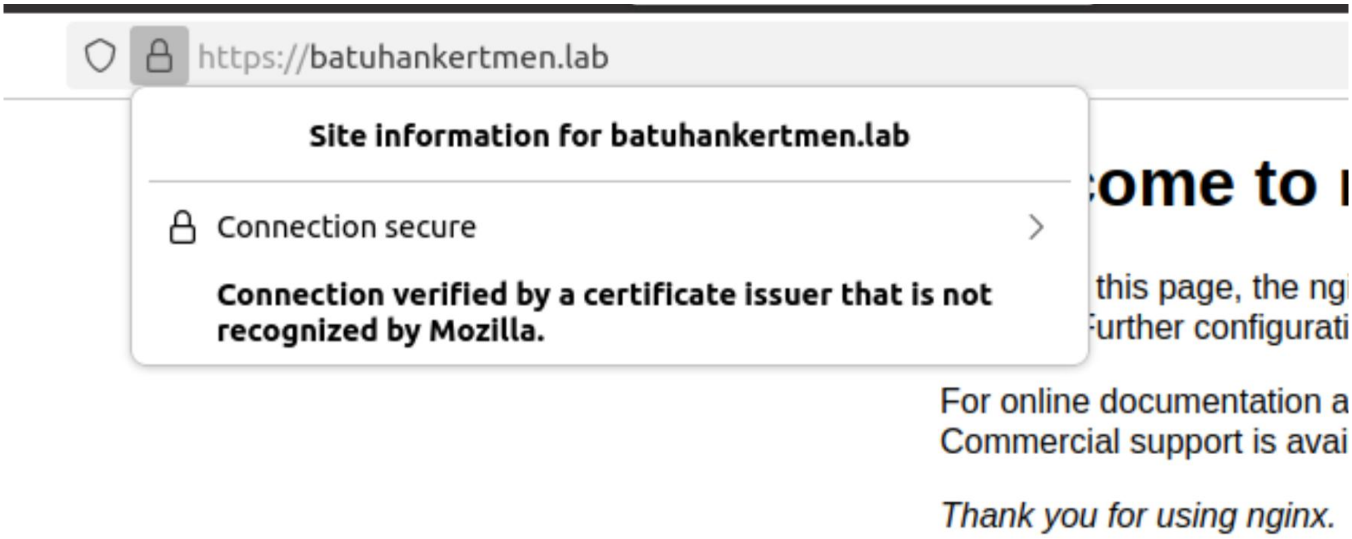
```
GNU nano 4.8
127.0.0.1       localhost
127.0.1.1       ubuntu
127.0.0.1       batuhankertmen.lab

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

What to Submit

Zip every file and name the file with your "*stuId_name_surname.zip*" (e.g. 34700_batuhan_kertmen.zip) and submit to suCourse.

- ca.key
- ca.crt
- server.key
- server.crs
- server.crt

Finally open your website in the browser and click on the lock icon in the address bar and take screen shot like the example below and add it to your zip file.



https://batuhankertmen.lab

Site information for batuhankertmen.lab

Connection secure

Connection verified by a certificate issuer that is not recognized by Mozilla.

come to n

this page, the ngi
Further configurati

For online documentation a
Commercial support is avai

Thank you for using nginx.