**Amanuel Reda**

**CECS 378**

**Screen Shot 1)** Right-click on the ca.crt file and Open with View file. Expand the details section and take a snip (screen shot) of the contents of the file and then close the file.

Graphical user interface, text, application

Description automatically generated

**Question 1)** How long is the ca.crt valid? What RSA key size was used for the Public key found in ca.crt?

**ANS:** 2048

**Question 2)** How many bits is the private key generated in the server.key?

**ANS:** 1024

**Question 3)** Who verified the server.crt certificate? How long is the server.crt valid?

**ANS:** csulb.edu verified the server.crt. The server.crt is valid for 365 days.

**Question 4)** Why do you think the web server failed to start when changing the certificate information but not the modulus information?

**ANS:** Because changing the certificate information makes the certificate invalid.

**Question 5)** Did your browser allow you to connect to the website? Why or why not?

NO

Unable to connect

Firefox can’t establish a connection to the server at localhost:4433.

The site could be temporarily unavailable or too busy. Try again in a few moments.

If you are unable to load any pages, check your computer’s network connection.

If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

**Task 4:**

**Question 6)** Did your browser allow you to connect to the website? Why or why not?

**ANS:** The browser didn’t allow me to connect to the websites, because they are not secured yet since we modified the victim’s /etc/hosts file.

Your connection is not secure

The owner of example.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

**Question 7)** How important is it to protect the private key of your CA? Explain…

**ANS:** Protecting the private key of my CA is very important. If it falls into the wrong hand, then someone can issue certificates fraudulently.

**Question 8)** What information is being stored in the index.txt file?

V 220916223529Z 1000 unknown /C=US/ST=California/L=Long Beach/O=SEEDLabs Inc./CN=SEEDPKILab2020.com

V 220917181814Z 1001 unknown /C=US/ST=California/L=Long Beach/O=Example Inc./

**ANS:** when we create a certificate, the database holds the certificates that are issued. Then, the index.txt file stores the indexes of those certificates. In this case, the index.txt file stored the indexes of the two certificates we have issued.

**Screen Shot 2)** Take a snip (screen shot) of your SEEDUbuntu1 desktop showing all the files and folders you created during this lab. Hint: Your screen shot should have 1 folder and 10 files.

A computer screen capture

Description automatically generated with low confidence