Sean Blanchard

5/14/2021

qanda

1. Submit your root-ca folder zipped up on Canvas.
2. db/index contains a database of certificates signed by your private CA. What does the first column mean? What are the possible values of the first column?

3 different possible values

1. Looking at the first certificate in your db/index, the third field is the serial number for the certificate. What is this numbers relationship to db/serial?

The relation looks to be that it takes the serial number and modifies the last two characters.

1. Looking at the serial number for the first certificate, can you find it in certs/? If so, which \*.crt file does it match in your root-ca directory?

My certs folder is empty.

1. We have revoked the last certificate due to key compromise. How will a browser know that the certificate is no longer valid?

It looks like it changed the serial number and added a note to be displayed.