Lab 2 - SSL Veritifcation and Validation

Submission Requirements

You must sumbit a zip file of your work above in a zip file that has the following structure. You should verify your lab submission to ensure you are sending me the correct work in the correct format in the correct directory and file structure. Many students have received a mark of zero for not submitting properly, not following the structure or simply submitting blank files/folders etc.

```
Lab2-shi-89/
    ├── Lab2-shi-89.md
    ├── SSLLabPart2-shi-89.txt
    └── img/
```

Purpose and Intent

The purpose of this lab is to farmiliarize the students with SSL handshaking and certificate validation.

Students must meet all submission requirements in order to receive marks for their lab.

Part 1 - SSL Validation

Find a website, using your web browser (you can pick any), validate the important parts of the certificate installation done.

Pick a website that uses SSL. Use the browser tools to prove the following important parts of the SSL configuration:

Take screenshots and highlight the revevant parts of the SSL configuration.

- SSL Certificate Chain
- SSL Certificate Serial Number
- SSL Certification Valid Start and End Dates

Part 2 - SSL Handshake

```
Remember you should provide the command you used in clear text as well as the
screenshot below.
```

Given the same website you did for Part 1, go ahead and use the `openssl` client on kali Linux to verify the steps of validation. Use the `s_client` option in openssl to view the SSL handshake (you will want to use the -vvv verbose flag).

1. Redirect the output into a text file using redirection in bash. Save the file as `SSLLabPart2.txt` and place it in your submission folder. Paste the command you used to do this in your markdown file.
2. Using Figure 22.6 (entitled: Handshake Protocol Action)in your textbook match the lines of the s_client output to the "phases" of the SSL connection. You can use a highlighting tool with to show each phase (be sure to highlight the entirity of the text, dont just use an ambigious arrow). Include the relevant comments to each phase explaining why they fall under which phase as well as a screenshot that highlights the text you are talking about.

Reflective Questions

```
Anwer the following reflection questions in your own words and include the answers
in your markdown file.
```

---

1. What protocol did the handshake negotiate? Why is this important?
2. Why do you think it is important to be able to use these diagnostic tools?
3. From a security perspective why is this information valuable?
4. What specific parts of the `s_client` output did you not understand, why?
5. What are valid SSL protocols that are currently safe to use? What are protocols that are deprecated? What does this mean? Why is it important?
