I. Heartbleed

- In your own words (and with proper citation when necessary), describe the function and purpose of the Heartbeat Extension for OpenSSL.
    - Originally, The Heartbeat Extension was meant to provide a protocol for TLS and removes the need for renegotiation and path discovery

- Again in your own words, describe the behavior of the Heartbeat Extension and the vulnerability that was discovered.
    - The Heartbleed bug had been exploited due to poor compatibility of the extension and was able to cause a leak of memory data that is being sent from server to client and vice versa
    - https://heartbleed.com/

- Describe how the vulnerability could be exploited and the impact of that exploitation. Pay particular attention to the topics we have covered in class.
    - The vulnerability had allowed anyone to view the systems' memory that were being protected using heartbreak. This had compromised the data that was being used on these sites such as private keys, usernames, emails, and passwords.

II. Extended Validation Certificate

In recent years, many secure websites have implemented Extended Validation Certificates (EV Certs)

- In a few sentences, define an EV Cert and how is it different that a standard (aka Domain Validation) certificate
    - An EV cert is the highest level certificate that can be granted. It ensures that the website is hosted from a secure place and the data on the site is secure.
- What are the criteria for issuing/acquiring an EV Certificate
    - For EV Authentication, there are many steps before the certificate can be acquired
        - EV Enrollment-Verifies that the applicant works for the org. That is applying for the certificate
        - Org. Auth.- Ensures that the Org. is legally registered and is active
        - Operational Existence- Proof that the Org. has existed for more than 3 years. If not, more documentation is required
        - Physical Address- Organization has a real physical address in the country of registration
        - Telephone Verification-Org. Has a working phone number
        - Domain Auth.-Verifies that the org. Owns the domain that is looking to be registered
        - Final verification call-CA calls the applicant to contact them about verification for the EV certification.

        - https://sectigo.com/resource-library/seven-steps-to-ev-ssl-issuance
- As a user how do you know that a site is using a different EV Cert? (different browsers may have their own methods of indication)
    - For Google Chrome, as well as many other browsers, within the URL search bar, there is a lock that can be clicked and the Cert info can be looked at. This can be used in order to follow the Auth of the Cert and see if it is an EV cert.
    -