10.2 Question 2

10.2.A Answer the following Questions

What security services are provided by TLS Record Protocol?

The TLS Record Protocol provides confidentiality by defining a shared secret key used for conventional encryption of the payloads. It also provides message integrity by defining a shared secret key which is used to form MACs.

Which of the following parameters correspond to session state and which to connection state?

Session State:
Peer Certificate, Cipher Spec, Master Secret
Connection State:
Server and Client Random, Server and Client write Keys, Server and Client MAC Secrets

***server_key_exchange* message in TLS Handshake protocol contains a digital signature of the exchanged server parameters and the random values from *client_hello* and *server_hello* messages. What is the purpose of signing these two random values?**

This is done in order to protect from replay attacks as a server should never allow a duplicate nonce, mitigating a capture and resending of a particular message.

Which certificate issue can you spot on https://bit.ly/3EwxKOt? Which TLS higher-level protocol takes care of sending certificate and other error messages?

The digital certificate issued is expired and therefore an error by the browser is raised. In TLS the Alert Protocol is used to inform the peer about the cause of a protocol failure.

10.2.B Match the following SSL/TLS attacks and describe how each of them can be mitigated.

CRIME .... Authentication cookie recovery thanks to the use of compression

Mitigation Options:
This approach can be defeated by preventing the use of compression at either the client end, the browser disabling the compression of HTTPS requests, or by the website preventing the use of data compression on such transactions using the protocol negotiation features of the TLS protocol. In TLS 1.2 it is specified that in the ClientHello message different compression methods can be specified and only one of these can be used during the communication between server and client (the messages are not compressed if no compression method is specified).

Bleichenbacher Attack .... Utilizes fixed PKCS#1 format and chosen-ciphertext weakness of RSA to decrypt pre_master_secret

Mitigation Options:
In order to mitigate a Bleichenbacher attack the RSA key exchange approach should be changed so that either DH or ECDH are used instead. Another option would be to use OAEP instead of PKCS. In the end the client should not be noticed about any Pre-Master decryption fails and the server should only inform the client once reaching the Finished State (as stated on https://datatracker.ietf.org/doc/html/rfc5246, p.60).

BEAST . . . . Chosen-plaintext attack on CBC mode encryption with chained IVs

Mitigation Options:
The easiest option to mitigate such an attack is to disable TLS 1.0 and 1.1 as well as SSL on the server.

"The Hacker's Choice"/DDoS Attack . . . . . Exploits SSL Renegotiation feature

Mitigation Options:
One can integrate an iRule which drops a connection of a client if he is renegotiating several times in a given time frame (i.e. 10 times in 1 minute). This drop will stall the attack for long periods of time which will fully negate the attack (see https://community.f5.com/t5/technical-articles/ssl-renegotiation-dos-attack-ndash-an-irule-countermeasure/ta-p/274560).