20% of overall Module

Due: Monday 11th December 2023 at 5pm

The aim of the project is to build a remote secure web site using HTTPS and WAMP/XAMP

DELIVERABLE

1. Live web site accessed using your public domain name. The default WAMP web page is not sufficient as your home page.
2. Two X.509 certificates signed by a CA (Certificate Authorities), e.g. ZeroSSL.
   (a) RSA certificate
   (b) EC (Elliptic Curve) certificate
3. Live **secure** (https) web site accessed using your domain name using each of the 4 cipher suites mentioned below.
4. Remote web site configured for following Cipher Suites
   a) TLSv1.3
   b) ECDHE-RSA-AES256-GCM-SHA384
   c) ECDHE-ECDSA-AES256-GCM-SHA384
   d) DHE-RSA-AES128-SHA (NB: change browser settings)
5. Wireshark trace for each of the 4 cipher suites.

Marks will be awarded for

1.	Live Website site on cloud, including live domain name	(20)
2.	Two X.509 certificates signed by a reputable CA	(10 each)
3.	Different Cipher Suites	
	i. TLSv1.3	(10)
	ii. ECDHE-RSA-AES256-GCM-SHA384	(10)
	iii. ECDHE-ECDSA-AES256-GCM-SHA384	(10)
	iv. DHE-RSA-AES128-SHA	(10)
4.	Video (between 10-15 minutes)	(35)
5.	Document detailing steps you followed	(25)
6.	Describing why there is no Certificate in TLS1.3 Wireshark trace	(25)

Marks are assigned under the following categories:

1. Functionality
2. Complexity
3. Originality
4. Completeness

Your submission **must** include:

1. A video *demonstrating* and *explaining* each of the above Cipher Suites using Wireshark. All elements of the cipher suite should be explained. This video is **your explanation** of the handshaking and record protocol used by TLS (Transport Layer Security).

2. A report outlining:
   - The steps you followed when implementing each different Cipher suite.
   - Screen shots of both certificates including path back to trusted root

3. Zip the files and call it '*Youname - Security*'.zip

Please note

This is an individual project. In the interest of fairness, integrity and equity for all students, I am not able to **do your assessment for you**. Instructional videos and written material have been provided on Moodle on how to complete this assessment.

Marks will be deducted for late submissions