Network Security

Spring 2018

Assignment 02-3 Due Date: 10th May 2018

Instructions:

- *The assignment must be submitted no later than **6.pm 10th May 2018**.*
- *Late assignments aren't going to be entertained*
- *You may use screenshots if necessary. You can even add a video of the code execution too.*
- *Naming of assignment folder: <reg.year>-<reg.number>-<first name>-<last name> e.g (15-5455-ibrahim-nadir). This should be format of both the root/main/principal folder and the main word/rtf/pdf file. Other programming related files must be in the format → <main-folder>/q1 and <main-folder>/q3 depending on the question.*
- *Where to submit: Submit it on the following link: https://drive.google.com/drive/folders/1l-X4iqIQAgLm74T6RZG22T8MAWAQy7uG?usp=sharing*
- *Failure in compliance to the format of submission will result in reduction of your score.*

Q 01. Use MD5 as the hash function and generate a collision practically using any programming language of your choice. Don't add the code in word file. Your code should be in a separate programming language file (e.g. MD5-collision.cpp). Put in a folder name "q1". How you run the code must be in a file named "readme.txt". What method you chose and how it works must be in the word file.

Q 02. Discuss what a heart-bleed bug attack is and how it can be fixed. The answer must be no longer than 350 words. Its accuracy and write up will decide your grade.

Q 03. A length-extension attack is one in which a hash algorithm is hacked such that data is appended to the original message and yet the hash is validated. Implemented such an attack on MD5 practically. Add the code in a separate folder named "q3". How you run the code must be in a file named "readme.txt". What method you chose and how it works must be in the word file.

Q 04. What is OWASP? Briefly explain briefly.

Q 05. What is DTLS (Datagram transport layer security)? How would you compare its success with SSL/TLS?

Q 06. Choose a web application of your choice (e.g. wordpress local website using wamp/xampp etc). Using any tool available in the Kali Linux you set up in previous assignment to brute-force the web application of your choice. Try different users and different passwords.

Bonus: Do a complete write-up on how would you break an RC4 encryption. Better yet if you can demonstrate it.(this will get you 11/10)