MCS 103 - Assignment 2 **MSc First Year 2018**

Date of Issue 10th September 2018 **Due Date 1st October 2018**

General Instructions

- Any programming language can be used for the implementation of both the Questions.
- Do it in groups of two/three but not in more than three
- CR will collect all the folders of all the groups in a pen-drive and submit it to me for evaluation maximum by 5pm.

Programming Instructions

- Note that all your programs should have proper alignment, indentation and proper comments.
- All constants / variables / functions etc. should have meaningful names.
- Overall, programs should be readable. If program fails to execute in the selected programming language, you will get zero for everything.
- Submission files – A2Q1_YourNames_RollNos.extension, A2Q1_YourNames_RollNos_readme.txt, A2Q2_YourNames_RollNos.extension, A2Q2_YourNames_RollNos_readme.txt, A2Q2_Name_RollNo_Folder (with test files)
- Read me files should give information about code, functions and data structures used, diagrammatic representation of the concepts, etc. You may refer to preparation of readme file from here.

Q1. Design an intelligent Intrusion Detection System (IDS) based on the various principles of Information Security. The system should intelligently select the features from the dataset, segregate the training dataset using clustering technique(s) (preferably K-Means) based on selected features, define properties of clusters formed, and predict whether the test data is case of an Intrusion or not.

Present an exhaustive analysis based on the results obtained through the designed IDS. You may use confusion matrix and statistical features to present the analysis.

Data Source

Data Description

Extra Points for

- *Using more than 2 clustering or classification techniques with their comparative analysis based on the results*
- *Creating Graphical Interface*
- *Self-implementation of data segregation techniques instead of using in-built functions*

Q2. Implement a system called “MyAntiVirus” to find potential Malware in your system.

Create a directory in your system with few files in it. This directory will work as the potential system for virus scanning through “MyAntiVirus”. Create technical codes (not necessarily working codes) in those files with software flaws like Infinite loop, incorrectly working loop, Memory overflow, Excessive usage of buffer space, Any prominent system call usage, Too much of unnecessary processing, etc. “MyAntiVirus” should be able to detect such files and give appropriate warnings.

“MyAntiVirus” should also be able to detect files in the system which have different/unusual functionality like varied execution time (Run slower than normal); unjustified behavior (Show popups both online and/or offline); Have codes that do not open, run slow or close unexpectedly; Opens-up an anonymous website on file execution; Show a blue screen with the error code; etc. These behaviors should be defined by you in the files which are detected by “MyAntiVirus”.

All the Best