

# Department of Computer Science

## COMP232 Individual coursework

### Assignment 3

Alexei Lisitsa  
a.lisitsa@liverpool.ac.uk

## 1 Overall marking scheme

The coursework for COMP232 consists of four assignments, contributing to 40% of the final mark. The contribution of the single assignments is as follows:

Assignment 1	10%
Assignment 2	10%
Assignment 3	20%
TOTAL	40%

Failure in any assignment may be compensated for by higher marks in other components of the module.

This document describes Assignment 3. Assignment 3 will be marked according to the following broad criteria:

- correctness of the answers;
- presence/absence of the evidence on the experiments;
- original contribution either in analysis or in presentation.

## Aims of the Assignment 3

- to illustrate the practical aspects of using Intrusion Detection Systems to secure legacy software;
- to test the students skills of using Snort IDS;
- to test the students skills in the analysis of the experiments.

# Securing Legacy Systems

This assignment asks you to follow the steps of Securing Legacy Systems-JHUISI instructions (DeterLab shared assignment considered in Labs 15-16) and perform all *Basic Tasks*. Please give a short description of the experiments you have done and answer all 12 questions in the Basic Task Section. These include:

- Questions 1-6 after **Start Snort Without Rules**,
- Questions 5-7 after the section **Analyze Network Traffic**, and
- Questions 8-10 after the section **Write Rules to Guard Against Simple Requests**.

## 2 Submission

You need to submit:

- Report (in \*.pdf, \*.doc, or \*.docx format)
- Any additional data/files asked for by the questions

The work must be submitted electronically via Electronic Coursework Submission System. This must be done by

**17.00 on Friday, 8th of May, 2020**

Please be aware that the standard University policies

- on plagiarism, collusion and fabricated data  
[www.liv.ac.uk/tqsd/pol\\_strat\\_cop/cop\\_assess/cop\\_assess.doc](http://www.liv.ac.uk/tqsd/pol_strat_cop/cop_assess/cop_assess.doc), Section 8 and
- on late submission  
[www.liv.ac.uk/tqsd/pol\\_strat\\_cop/cop\\_assess/cop\\_assess.doc](http://www.liv.ac.uk/tqsd/pol_strat_cop/cop_assess/cop_assess.doc), Section 6

are applied to this assignment.