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:

<table>
<thead>
<tr>
<th>Assignment</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assignment 1</td>
<td>10</td>
</tr>
<tr>
<td>Assignment 2</td>
<td>10</td>
</tr>
<tr>
<td>Assignment 3</td>
<td>10</td>
</tr>
<tr>
<td>Assignment 4</td>
<td>10</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>40</strong></td>
</tr>
</tbody>
</table>

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 14-15) 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.

Note

Please note that during the Easter break the Departments Labs will be closed. You can however access your Deterlab accounts from anywhere using your browser and perform experiments if you wish. In non-Linux systems you can use SSH clients easily available for other platforms (e.g. PuTTY for Windows).

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, 3rd of May, 2019

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

- 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.