**FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE**

Supervisor's statement of a final thesis

Supervisor: Ing. Alexandru Moucha, Ph.D.
Student: Jakub Šimůnek
Thesis title: Architektura a technologie bezpečnostního dohledového
                            centra (SOC)
Branch / specialization: Computer Security and Information technology
Created on: 30 January 2024

Evaluation criteria

1. Fulfillment of the assignment

▸ [1] **assignment fulfilled**
  [2] assignment fulfilled with minor objections
  [3] assignment fulfilled with major objections
  [4] assignment not fulfilled

The work fulfills the requirements, in fact I myself learned new things from its content, as it will be explained in the final words.

2. Main written part   90 / 100 (A)

The written part is clear, well organised, easy to read and understand. The student submitted periodic iterations which allowed on-the-fly improvements of it.

3. Non-written part, attachments   85 / 100 (B)

The testing rig was rather simplistic, however enough for a proof of concept. This is expected as most probably the student is not allowed to have permission to deploy such tools in a live, production network nor that he owns an infrastructure large enough for further, in-depth-tests.

4. Evaluation of results, publication outputs and awards   90 / 100 (A)

The thesis came as an idea from the student - most probably he was interested as part of his work or hobby - and I realised that I can also apply its content as part of my own infrastructure, which became large enough such that it requires automatic monitoring. Thus, although the results are not containing elements of novelty which may be published, the work itself may be used a guideline for anybody who needs a reliable, cheap and rather good system to monitor his network. The used applications are free to

use (at least to a certain extent) and this is a very positive for someone who is not oriented towards a certain provider of equipment and monitoring solutions which may become extremely expensive even for large enterprises (e.g. Cisco).

5. Activity of the student

▸ [1] **excellent activity**
   [2] very good activity
   [3] average activity
   [4] weaker, but still sufficient activity
   [5] insufficient activity

The student constantly updated me to the progress of the work, overall I was very satisfied with his work and outcome.

6. Self-reliance of the student

▸ [1] **excellent self-reliance**
   [2] very good self-reliance
   [3] average self-reliance
   [4] weaker, but still sufficient self-reliance
   [5] insufficient self-reliance

I did not impose to the student a certain methodology / approach or applications, thus all the discovered tools, their interconnection and testing are his own artefacts.

The overall evaluation   90 /100 (A)

It is clear that I was very satisfied with the outcomes of the work. They allowed me to also evaluate my own monitoring tools. As I already mentioned, the work may be used by anybody who needs constant monitoring and security assessment of his own infrastructure, at least as a starting point. The cost of the implementation is zero or close to zero.

Instructions

Fulfillment of the assignment

Assess whether the submitted FT defines the objectives sufficiently and in line with the assignment; whether the objectives are formulated correctly and fulfilled sufficiently. In the comment, specify the points of the assignment that have not been met, assess the severity, impact, and, if appropriate, also the cause of the deficiencies. If the assignment differs substantially from the standards for the FT or if the student has developed the FT beyond the assignment, describe the way it got reflected on the quality of the assignment's fulfilment and the way it affected your final evaluation.

Main written part

Evaluate whether the extent of the FT is adequate to its content and scope: are all the parts of the FT contentful and necessary? Next, consider whether the submitted FT is actually correct – are there factual errors or inaccuracies?

Evaluate the logical structure of the FT, the thematic flow between chapters and whether the text is comprehensible to the reader. Assess whether the formal notations in the FT are used correctly. Assess the typographic and language aspects of the FT, follow the Dean's Directive No. 52/2021, Art. 3.

Evaluate whether the relevant sources are properly used, quoted and cited. Verify that all quotes are properly distinguished from the results achieved in the FT, thus, that the citation ethics has not been violated and that the citations are complete and in accordance with citation practices and standards. Finally, evaluate whether the software and other copyrighted works have been used in accordance with their license terms.

Non-written part, attachments

Depending on the nature of the FT, comment on the non-written part of the thesis. For example: SW work – the overall quality of the program. Is the technology used (from the development to deployment) suitable and adequate? HW – functional sample. Evaluate the technology and tools used. Research and experimental work – repeatability of the experiment.

Evaluation of results, publication outputs and awards

Depending on the nature of the thesis, estimate whether the thesis results could be deployed in practice; alternatively, evaluate whether the results of the FT extend the already published/known results or whether they bring in completely new findings.

Activity of the student

From your experience with the course of the work on the thesis and its outcome, review the student's activity while working on the thesis, his/her punctuality when meeting the deadlines and whether he/she consulted you as he/she went along and also, whether he/she was well prepared for these consultations.

Self-reliance of the student

From your experience with the course of the work on the thesis and its outcome, assess the student's ability to develop independent creative work.

The overall evaluation

Summarize which of the aspects of the FT affected your grading process the most. The overall grade does not need to be an arithmetic mean (or other value) calculated from the evaluation in the previous criteria. Generally, a well-fulfilled assignment is assessed by grade A.