FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Student:	Petr Heřmánek
Reviewer:	Ing. Tomáš Zahradnický, Ph.D.
Thesis title:	The Stack Clash Attack
Branch of the study:	Information Technology

Date: 9. 6. 2018

Evaluation criterion: *The evaluation scale: 1 to 4.*

1. Fulfilment of the assignment

1 = assignment fulfilled,
2 = assignment fulfilled with minor objections,
3 = assignment fulfilled with major objections,
4 = assignment not fulfilled

Criteria description:
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.

Comments:

I consider the topic of the thesis as fulfilled.

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

2. Main written part

65 (D)

Criteria description:
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. 26/2017, 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.

Comments:

The thesis meets criteria for a bachelors thesis.

The two overview chapters are in my opinion unnecessarily long and contain inaccurate statements from computer architectures and operating systems such as:

1. "The address space of each process is private and cannot be accessed by other processes unless it is shared." Only portions of the address space are shared, at page level, not address space as a whole.
2. "...program counter determining executed instructions". The program counter register contains the address of the instruction being executed.
3. Page 4 section 1.3 - "Numerous processors also use memory storage ... - the processor registers".

Shellcode is confused with generic exploit code. Shell code is a special kind of exploit with purpose to run a shell. Thus its name.

The end of the thesis where other platforms should have been be discussed is brief.

I have no objections to typography and language of the thesis.

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

3. Non-written part, attachments

100 (A)

Criteria description:
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.

Comments:

The attachment flash disk is nicely prepared with everything documented and commented, including a VirtualBox appliance.

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

4. Evaluation of results, publication outputs and awards

85 (B)

Criteria description:
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.

Comments:

The thesis demonstrates the Stack Clash attack on an older 32-bit architecture, which are nowadays rare. The thesis could still be used for didactic purposes. I have found it on the BI-BEK course website. I am wondering, why it is written in English, as Czech would benefit most students of the course better than English.

Evaluation criterion: *No evaluation scale.*

5. Questions for the defence

Criteria description:
Formulate questions that the student should answer during the Presentation and defence of the FT in front of the SFE Committee (use a bullet list).

Questions:

1. Page 4 section 1.3 writes: "Numerous processors also use memory storage ... - the processor registers". This sentence suggests that only some processors have registers. Can the student elaborate this?
2. The architecture chosen by the student is obsolete as a whole. Why did not he try to compare it, at least, with the current operating systems?

Evaluation criterion: *The evaluation scale: 0 to 100 points (grade A to F).*

6. The overall evaluation

75 (C)

Criteria description:
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.

Comments:

I do hereby recommend the bachelors thesis of Mr. Petr Hermanek for defence and grade it with C (Good).

Signature of the reviewer: