Review report of a final thesis

Czech Technical University in Prague **Faculty of Information Technology**

Student:	Mr Alejandro Robledo
Reviewer:	Mgr. Rudolf Bohumil Blažek, Ph.D.
Thesis title:	Network Time Protocol attacks detection
Branch of the study:	Computer Security

Date: 9. 6. 2016

Evaluation criterion:	*The evaluation scale: 1 to 5.*
1. Difficulty and other comments on the assignment	*1 = extremely challenging assignment,* *2 = rather difficult assignment,* ***3 = assignment of average difficulty,*** *4 = easier, but still sufficient assignment,* *5 = insufficient assignment*

Criteria description:
Characterize this final thesis in detail and its relationships to previous or current projects. Comment what is difficult about this thesis (in case of a more difficult thesis, you may overlook some shortcomings that you would not in case of an easy assignment, and on the contrary, with an easy assignment those shortcomings should be evaluated more strictly.)

Comments:
The thesis deals with implementing and testing chosen detection methods for selected attacks on the NTP protocol. Therefore I consider the assignment to be of average difficulty.

Evaluation criterion:	*The evaluation scale: 1 to 4.*
2. 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 thesis meets the assignment statement. In Comments indicate parts of the assignment that have not been fulfilled, completely or partially, or extensions of the thesis beyond the original assignment. If the assignment was not completely fulfilled, try to assess the importance, impact, and possibly also the reason of the insufficiencies.

Comments:
All assigned goals were addressed and met in the thesis.

Evaluation criterion:	*The evaluation scale: 1 to 4.*
3. Size of the main written part	***1 = meets the criteria,*** *2 = meets the criteria with minor objections,* *3 = meets the criteria with major objections,* *4 = does not meet the criteria*

Criteria description:
Evaluate the adequacy of the extent of the final thesis, considering its content and the size of the written part, i.e. that all parts of the thesis are rich on information and the text does not contain unnecessary parts.

Comments:
The presented work satisfies the requirements on the scope and breadth of an M.Sc. diploma thesis, and all its parts are appropriately detailed.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
4. Factual and logical level of the thesis	*88 (B)*

Criteria description:
Assess whether the thesis is correct as to the facts or if there are factual errors and inaccuracies. Evaluate further the logical structure of the thesis, links among the chapters, and the comprehensibility of the text for a reader.

Comments:
The logical structure of the thesis is acceptable, and the thesis does not contain any serious factual errors.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*90 (A)*

Criteria description:
Assess the correctness of formalisms used in the thesis, the typographical and linguistic aspect s, see Dean's Directive No. 12/2014, Article 3.

Comments:
The formal and typographical aspects of the thesis are appropriate and without any excessive errors.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
6. Bibliography	*60 (D)*

Criteria description:
Evaluate the student's activity in acquisition and use of studying materials in his thesis. Characterize the choice of the sources. Discuss whether the student used all relevant sources, or whether he tried to solve problems that were already solved. Verify that all elements taken from other sources are properly differentiated from his own results and contributions. Comment if there was a possible violation of the citation ethics and if the bibliographical references are complete and in compliance with citation standards.

Comments:
The use of references to literature is acceptable, citations are used appropriately in the Analysis chapter. However, is some areas citations are missing. E.g. Section 3.3. on offset-based detection does not explain who proposed the method. The main problem is, that some figures in the thesis use pictures from other works without citing the source. E.g. Fig. 1.1 is taken from WikiPedia without giving proper credit. This approach to using other works is not acceptable.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
7. Evaluation of results, publication outputs and awards	*85 (B)*

Criteria description:
Comment on the achieved level of major results of the thesis and indicate whether the main results of the thesis extend published state-of-the-art results and/or bring completely new findings. Assess the quality and functionality of hardware or software solutions. Alternatively, evaluate whether the software or source code that was not created by the student himself was used in accordance with the license terms and copyright. Comment on possible publication output or awards related to the thesis.

Comments:
The detection methods implemented in the thesis were partially tested. After more thorough testing, the results of the thesis have the potential to be published in a conference paper about the NEMEA system.

Evaluation criterion:	*No evaluation scale.*
8. Applicability of the results	

Criteria description:
Indicate the potential of using the results of the thesis in practice.

Comments:
The developed module can be used as a part of CESNET's NEMEA system that is targeted at practical deployment to improve the security of computer networks and systems. The module has thus the potential to be practically beneficial for the IT community.

Evaluation criterion:	*No evaluation scale.*
9. Questions for the defence	

Criteria description:
Formulate any question(s) that the student should answer to the committee during the defence (use a bullet list).

Questions:
- How did you evaluate the performance of the detection algorithm after you determined the thresholds? Did you measure false alert occurrences? Did your measure detection success rates, detection delays, or some similar metric?

- How difficult would it be to perform a large testing experiment with randomized previously captured NTP data and randomly initiated attacks?

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
10. The overall evaluation	*89 (B)*

Criteria description:
Summarize the parts of the thesis that had major impact on your evaluation. The overall evaluation **does not** have to be the arithmetic mean or any other formula with the values from the previous evaluation criteria 1 to 9.

Comments:
The thesis implements interesting detection methods that will contribute to the functionality of CESNET's NEMEA system. After more testing the module has the potential to be practically useful. I am reducing the grade to B for using other works (figures) inappropriately.

Signature of the reviewer: