Supervisor's statement of a final thesis

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

Student:	Mr Alejandro Robledo
Supervisor:	Ing. Tomáš Čejka
Thesis title:	Network Time Protocol attacks detection
Branch of the study:	Computer Security

Date: 5. 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:
This thesis topic belongs to difficult ones since it deals with non-trivial NTP vulnerability that can be exploited by attackers to manipulate with victim's system time.
The tasks of the thesis contained verification of the attack repeatability in a virtual environment, analysis of the traffic generated by attackers, design of detection mechanism and implementation of detection module.

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:
The student prepared virtual laboratory consisting of virtual machines. This laboratory was used for experiments. After analysis and design phase, the student extended an open-source flow exporter in order to obtain application specific information needed for detection. Finally, the whole monitoring and analysis pipeline was tested and verified.

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 thesis document fulfills all requirements.

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

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 thesis is logically structured, it contains all relevant and needed parts. The thesis contains description and explanation of Network Time Protocol (NTP), whereas this knowledge is the basic building stone in order to design functional detection module. The thesis also describes principles of the detected attacks that targets NTP clients.

Evaluation criterion:	*The evaluation scale: 0 to 100 points (grade A to F).*
5. Formal level of the thesis	*89 (B)*

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 text contains some typographic mistakes and misspellings, however, the understanding is not affected at all. The thesis is easily readable and, as far as I can grade it, it is well-written in English.

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

6. Bibliography	*90 (A)*

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 student found enough references that are related to this topic. References list contains some online sources as a complement to official published documents and specification.

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

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:
This thesis is a valuable contribution for a world-wide community of network security. The topic was clearly described in the thesis document, the student created an environment that allows for evaluation of NTP vulnerability as well as testing developed detection module. The results of the thesis, i.e. NTP plugin for open-source flow exporter and the detection module are going to be published at the official repository of the NEMEA project. In addition, the thesis was rewritten and submitted as a paper for the international Prague Embedded Workshop 2016.

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 results of this thesis are a valuable contribution for analysis of NTP traffic of small computer networks and the detection module can be easily deployed in order to detect suspicious behavior that can lead to affecting victim's system time.

Evaluation criterion:	*The evaluation scale: 1 to 5.*
9. Activity and self-reliance of the student	*9a:* ***1 = excellent activity,*** *2 = very good activity,* *3 = average activity,* *4 = weaker, but still sufficient activity,* *5 = insufficient activity* *9b:* ***1 = excellent self-reliance,*** *2 = very good self-reliance,* *3 = average self-reliance,* *4 = weaker, but still sufficient self-reliance,* *5 = insufficient self-reliance.*

Criteria description:
Review student's activity while working on this final thesis, student's punctuality when meeting the deadlines and consulting continuously and also, student's preparedness for these consultations. Furthermore, review student's independency.

Comments:
The student visited all meetings, he was well-prepared, he came up with valuable ideas that led to the solution of issues.

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

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 topic was fulfilled and the results are an excellent contribution for the NEMEA project. From my opinion, the topic can be a great starting point for additional research in the network security area.

Signature of the supervisor: