THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	Evading CAPE Sandbox Detection
Author's name:	Ondřej Maňhal
Type of thesis :	Master Thesis
Faculty/Institute:	Faculty of Electrical Engineering
Department:	Department of Computer Science
Thesis reviewer:	Sebastian Garcia
Reviewer's department:	Department of Computer Science

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **D**

How demanding was the assigned project?

The assignment was somehow demanding in the sense that it required thinking how CAPEv2 could be evaded and implemented some attacks

Fulfilment of assignment **C**

How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.

The thesis fulfils the assignment enough to be interesting and to provide some new insight on how CAPEv2's monitoring system can be evaded. The goal is fulfilled in the sense of finding if the monitor system could be evaded, which it can. However, the complete spectrum of all the techniques that could evade the monitor system and why they can evade it was not completely explored, leaving some avenues unexplored.

Methodology **E**

Comment on the correctness of the approach and/or the solution methods.

Even though the technique used was good, the methodology of research could have been much better. In particular there were issues with the definition of the goal, the previous work research, the description of the steps, the documentation and the comparison and evaluation. However, the results are useful and will be used by the community.

Technical level **C**

Is the thesis technically sound? How well did the student employ expertise in the field of his/her field of study? Does the student explain clearly what he/she has done?

The thesis is technically sound and the student used the expertise correctly to implement known techniques of attacks. However, sometimes the work is not completely clearly described and some experiments are not documented properly.

CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE

THESIS REVIEWER'S REPORT

Formal and language level, scope of thesis	**B**
Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?	
The formalisms are used properly and the thesis is organised in a logical way. The thesis is presented in an understandable and logical way showing the research done. The language is clear and the English satisfactory.	

Selection of sources, citation correctness	**C**
Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?	
The thesis does reference some earlier work but I would have liked some more exploration in other previous work doing evasion of sandboxes. The work analysis of the student is original and the citations are correct.	

Additional commentary and evaluation (optional)

Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.

The student presented a research on how to evade the monitoring capabilities of the CAPEv2 sandbox using attacks done by the metasploit framework on persistence, privilege escalation and other type of attacks. Such knowledge is needed to better understand the limitations of CAPEv2, and to know how the community can improve our tools. The biggest weakness of the thesis is the lack of a good methodological research process. In particular there is a need for a better defined goal (together with a measurement if it was completely fulfilled), better previous work on other work escaping sandboxes, better design and documentation of experiments, and a comparison of the results with other techniques or previous papers. Even though the work done, these issues decrease the value of the thesis.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

Summarize your opinion on the thesis and explain your final grading. Pose questions that should be answered during the presentation and defense of the student's work.

The grade that I award for the thesis is **D.**

The thesis is on a topic that is important and relevant: the evasion of monitoring in a sandbox that could be abused by malware. The attacks done with metasploit are relevant and explore the limitations of CAPEv2, which seems to need to be improved to catch up with these problems. However the thesis lacked some methodological structure that made some findings difficult to asses, and in general made the thesis need a more research structure. This lack of research validation and exploration left some things that could be improved.

Date: **2022/06/12** Signature: