THESIS SUPERVISOR'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Evade CAPE Sandbox Detection**
Author's name:	**Ondrej Manhal**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Computer Science
Thesis reviewer:	Thorsten Sick
Reviewer's department:	External, Avast

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

How demanding was the assigned project?

Cape and Metasploit are both complex and tricky projects. They are not meant to be operated by unskilled people. Networking, Network interception, Windows internals (process hooking). And all of that is based on a Linux PC. Metasploit is a Pen testing tool for people who want to operate a system beyond the designed and implemented boundaries. Metasploit is also very tricky to run successfully. Programming was not relevant. But some debugging and reading of code was. The required languages were C, Python and Ruby.

Fulfilment of assignment **fulfilled**

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 system for experiments was properly set up. Several experiments were designed based on the understanding of the underlying systems (gathered from documentation and reading source code). The experiments were run, documented. Learnings were gathered and shared with the CAPE developers. The student experimented with a mixture of CAPE bypass mechanisms; some were successful.

Activity and independence when creating final thesis **A - excellent.**

Assess whether the student had a positive approach, whether the time limits were met, whether the conception was regularly consulted and whether the student was well prepared for the consultations. Assess the student's ability to work independently.

Ondrej gained full independence during the thesis. Especially when debugging a network error caused by broken CAPE hooking, cross verifying findings with an official CAPE version (to exclude own configuration mistakes as a cause) and coming up with interesting ways to circumvent detection.

Technical level **A - excellent.**

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

It is technically sound. Everything relevant was explained and a large number of skills were required to get to those results.

Formal level and language level, scope of thesis **A - excellent.**

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 language is clear and understandable. Citations are there. The structure is extremely well done. Basics for the technical reader without security skills were introduced first, then the tools were described. Background on special topics that are relevant like process injection was next. At the end of the thesis the experiments and results are described in a way that they can be reproduced without wasting the time of the reader.

Selection of sources, citation correctness	**A - excellent.**
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?	
All claims are supported by citations, many of them to source code, blogs and similar – which is expected in this field. Because CAPE and Metasploit are very centered in the hacking community and this type of literature are adequate for citation because the hacking community is using specifically these to discuss new learnings (instead of e.g. papers in scientific journals). Citation style: I cannot judge this as I do not know the CTU specific style guide.	

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.
This thesis and similar follow up works can have a significant practical impact on the field. Real world attacks are moving towards file-less attacks using Metasploit. Many security teams use sandboxes (either CAPE or similar) for analysis of an attack. Knowing the weaknesses in analyzing those attacks or maybe even fixing some issues in those sandboxes is essential to continuing malware and attack analysis on the current quality level. It was relevant for the success that the student tried several quite different approaches to circumvent the CAPE monitor and covered a large area of the field of potential attacks.

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

In addition to everything written I enjoyed that the student gained independence and momentum in the course of his research as soon as we defined the boundaries of the research and learned the inner workings of the tools together. The last view sync meetings I was just curious asking myself "what did he try this time and did he succeed?". It was interesting and I learned a lot.

The grade that I award for the thesis is **A - excellent.**

Date: **1.6.2022** Signature: