FACULTY
OF INFORMATION
TECHNOLOGY
CTU IN PRAGUE

Review report of a final thesis

Reviewer:	Mgr. Peter Kálnai, Ph.D.
Student:	Bc. Matěj Havránek
Thesis title:	Attacks on Event Tracing for Windows: Techniques and Countermeasures
Branch / specialization:	Computer Security
Created on:	4 June 2023

Evaluation criteria

1. Fulfillment of the assignment

- ▸ [1] **assignment fulfilled**
- [2] assignment fulfilled with minor objections
- [3] assignment fulfilled with major objections
- [4] assignment not fulfilled

The student fulfilled the aims of the FT and implemented the practical goals, all in adequate quality.

2. Main written part 90/100 (A)

The FT follows the Dean's Directive No. 58/2023, Article 3. The structure of the thesis is appropriate. The citation ethics has not been violated.

The theoretical part, Chapter 1, contains mostly the description of the Event Tracing for Windows. The author successfully managed to describe such complex framework in a dense and compact form. However, an improvement in readability would be further connecting the abstract components of ETW with concrete applications, for example to mention that the tools from Section 1.6 are basically ETW controllers, or explain why some ETW sessions are called system loggers from certain point.

Next, Chapter 2 is the analytical part and contains the description of various types of attacks targeting ETW. It expands already published results, to which the student actively contributed.

Finally, Chapter 3 and Chapter 4 serve as a high-level documentation for the practical part. Chapter 3 also contains the comparison of two states, before and after the execution of the ETW attacks.

There are only a few typos and errors in the text, for example the first sentence of the Section 1.3.1 (page 12) or the link for the CVE-2023-21753 reference (page 87).

3. Non-written part, attachments 100/100 (A)

This part of the FT includes mainly the user- and kernel-mode detectors written in Python and C++, respectively. The programs are functional and the quality is very satisfying. The empirical value of 4 detected anomalies in the Python detector seems appropriate.

Moreover, the author successfully implemented a proof-of-concept, ETW Blinder, demonstrating the discussed ETW attacks.

4. Evaluation of results, publication outputs and awards 100/100 (A)

The results from this FT add new findings to the current knowledge about possible attacks against ETW and may attract the attention of experts in the field. The author's contribution on the mitigation side could be the basis of additional research and development, that may be useful even for practical applications.

The overall evaluation 99/100 (A)

The student had to face three tasks, all of which are far from being simple: to study and understand the complex ETW framework; to analyse and re-implement some of ETW attacks with the help of little documented Windows internals; to design and implement user- and kernel-mode detectors of such attacks. Overall, the assignment was fulfilled very well.

Questions for the defense

1) There is one system logger with ID 0x02 mentioned on page 77. Could this be Circular Kernel Context Logger?
2) Why there are two sections "Attacks on ETW" (1.8 and the whole Chapter 2)? What were reasons behind not to completely separate the theory around ETW in the Chapter 1 and the types of related attacks in the Chapter 2?
3) How big portion of the pywintrace/etw module is leveraged by the Python detector? Have you considered to implement it as a self-contained, stand-alone tool?

Instructions

Fulfillment of the assignment

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.

Main written part

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. 52/2021, 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.

Non-written part, attachments

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.

Evaluation of results, publication outputs and awards

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.

The overall evaluation

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.