Exercise sheet 02

Submit individually (1 person) or as a group (max. 3 persons).

1. Access control implementation: access control lists

How are access control lists (DACL) evaluated in Microsoft Windows?

1. How is the special case NULL DACL treated?
2. How is the special case empty DACL treated?
3. In what order are ACEs processed?
4. Because of the order in which ACEs are processed – in which order should you store allow ACEs and deny ACEs? Why?
5. What privileges make a DACL ineffective as a protection mechanism and why?

2. Access control implementation: tokens

Every process/thread in Windows is assigned a token. When access by a subject to an object is checked, the contents of the token are compared with the contents of the access control list.

1. Name the Security identifiers (SIDs) that are included in a token.
2. When is group membership determined?
3. What is the purpose of restricted SIDs in a token?
4. Give an example when you use a restricted token for a child process/thread.

3. Unknown real-world software vulnerabilites

3.1. Download the source code for the Moodle learning management system: https://moodle.org/

3.2. What are assets protected by Moodle? What are protection goals for the individual data items/assets on the server in terms of confidentiality, integrity, authenticity, and availability? Be specific in your answer and supply examples (in addition).

3.3. Since you will probably not be able to inspect the whole source code, what strategy do you choose to inspect only parts of the source code? Why do you choose that strategy?

3.4. Based on the specific assets that you identified in 3.2 that need protection, determine the parts of the source code of Moodle that are within the scope of your inspection.

Answers must be submitted in Moodle as a single PDF file following the naming convention:
Exercise02-YourLastName-YourFirstName.pdf
Example: Exercise02-Mustermann-Erika.pdf
For groups, the submission must include names and student numbers of all group members and the naming convention for the pdf file is different:
Exercise02-YourLastName1-YourLastName2-YourLastName3-YourLastName4.pdf
Example: Exercise02-Schmidt-Mueller-Meier-Schulze.pdf