Exercise sheet 01

Submit individually (1 person) or as a group (max. 3 persons).
Use of Generative AI is not permitted for this exercise sheet.
Include your name on the first page of your submission pdf file.

1. Web Application Vulnerabilities (Without Time Constraints)

1.1. Create an account with root-me.org.
1.2. Solve 2 of the challenges in the category Challenges => Web-Client that have a name starting with "XSS". [Groups: 2 challenges per group member, e.g., 6 challenges for 3 persons]
1.3. Solve 5 of the challenges in the category Challenges => Web-Server that have a name starting with "HTTP". [Groups: All challenges starting with “HTTP”]
1.4. Document for each challenge what you did, what tools you used, what worked and what did not work.

2. Access Control Implementation: Access Control Lists

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

2.1. How is the special case NULL DACL treated?
2.2. How is the special case empty DACL treated?
2.3. In what order are ACEs processed when an ACL is parsed for matching ACEs?
2.4. Because of the order in which ACEs are processed – in which order should you store allow ACEs and deny ACEs? Why?
2.5. What system-wide privileges make a DACL ineffective as a protection mechanism and why?

3. 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.

3.1. Name the security identifiers (SIDs) that are included in a token.
3.2. Group membership of a subject is checked at the time of token creation. Discuss this design decision both from a security and a runtime performance perspective.
3.3. What is the purpose of restricted SIDs in a token?
3.4. Give an example when you should use a restricted token for a child process/thread.

Answers must be submitted in Moodle as a single PDF file following the naming convention:
Exercise01-YourLastName-YourFirstName.pdf
Example: Exercise01-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:
Exercise01-GROUP-YourLastName1-YourLastName2-YourLastName3-YourLastName4.pdf
Example: Exercise01-GROUP-Schmidt-Mueller-Meier-Schulze.pdf
All group members must submit an identical pdf file in Moodle. E.g., 3 group members, 3 uploads.