Exercise Sheet 01

Individual submissions only. Talk, discuss, debate. Write separately **in your own words**.
If you use Generative AI, you need to document which AI tool you use and all the prompts. You are still fully responsible for the correctness of your submission.
Include your name on the first page of your submission pdf file.

1. User Authentication: Passwords

HTWG has ca. 5,000 user accounts that are protected by passwords chosen by users. Each password needs to be at least 14 characters long. Assuming that users prefer simple passwords that are exactly 14 characters long, how many different passwords are possible when users only use lower case characters a..z for their passwords?

1.1. An attacker might perform an *online attack* on the passwords of HTWG's users. Assume that the probability of all passwords is equal. Assume further that the attacker can try **40,000 different passwords per second**. How many *days* in total does the attacker have to guess passwords until the attacker guesses the correct password for a specific account? Explain your calculation ("Rechenweg"). Remember: The unit is *days*.

1.2. Assume that the probability of passwords is not equal. Assume that 90% of the users choose their passwords from a set of 1,000 popular passwords. Assume further that the attacker can try 5**,000 different passwords per second**. How many *seconds* on average does the attacker have to guess passwords until the attacker guesses the correct password for at least 90 accounts? Explain your calculation ("Rechenweg"). Remember: The unit is *seconds*.

1.3. Assume that a) the attacker can only perform an online attack against one specific account (you do not know in advance which one), and b) that 90% of the users choose their passwords from a set of 1,000 popular passwords. Assume further that you want the attacker to be unsuccessful with a probability of 60%. **After how many tries** do you need to shut down the authentication mechanism? Explain.

2. Accesss Control

Restricting access by people/accounts/programs ("subjects") to resources ("objects") is a method to preserve confidentiality, integrity, and availability of objects. There are different approaches how you can define who can perform which actions on what.

2.1. Pick three apps on your smartphone. What is the purpose of each app and what permissions are associated with these apps? Is the association of permissions with apps an access control list or a capability list? Why?

2.2. Explain how role-based access control works. Use Moodle as an example for an application that uses role-based access control.

3. Application Whitelisting

Get familiar with built-in techniques for **application whitelisting in Microsoft Windows**.

3.1. Explain how application whitelisting works with **WDAC (Windows Defender Application Control)**?

3.2. Does WDAC restrict users/processes with respect to executing code? How?

3.3. Does WDAC restrict users/processes with respect to reading and writing files? How?

3.4. What are the different **file rules** hat you can use with WDAC?

3.5. What is the purpose of the **audit mode** in WDAC?

3.6. How do you debug WDAC policies, i.e., how do you find out that they are effective and where are WDAC events logged?

Answers must be submitted in Moodle as PDF files following the naming convention:
Exercise01-YourLastName-YourFirstName.pdf
Example: Exercise01-Mustermann-Erika.pdf