Exercise sheet 02

Individual submissions only. Talk, discuss, debate. Write separately **in your own words**.

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, how many different passwords exist 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 **200 different passwords per second**. How many *hours* in total does the attacker have to guess passwords until the attacker guesses the correct password for a specific account? Explain your calculation ("Rechenweg").

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 **200 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 100 accounts? Explain your calculation ("Rechenweg").

1.3. Assume that a) the attacker can only perform an online attack against one specific account, 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 99%. After how many tries do you need to shut down the authentication mechanism? Explain.

1.4. Now consider an *offline attack*. Assume still that users limit their passwords to 14 characters out of an alphabet of 26 lower case characters. How many passwords does an attacker need to hash per second if the attacker should be able to hash only 50% of all possible user passwords in 2 years. Consider a) speed needed when salting is not used, and b) speed needed then salting is used. Explain your calculations ("Rechenweg").

2. Accesss rights in file system

IT-Grundschutz recommends that users should not be allowed to execute programs that are stored in directories for which users have write access (requirement SYS.2.2.2.A14). The reason is that these programs might have been downloaded by users and are not trustworthy. For a simple group policy that could be applied, you need to identify directories for which users have read access only.

1. For a computer running Microsoft Windows, **in which directories can users write files**? If your directory tree is too large, you can leave out subdirectories if users have write access both for a directory and all its subdirectories. E.g., if users can write in C:\foo and C:\foo\bar and C:\foo\contoso and if bar and contoso are the only subdirectories of foo, it is sufficient to just report C:\foo instead of C:\foo, C:\foo\bar, C:\foo\contoso.
   If you do not have access to a computer running Microsoft Windows, use one of the Windows computers in a pc-pool or set up a virtual machine with Microsoft Windows.
   The tool *AccessChk* from Sysinternals might be helpful. Document all the steps you take, do not only present a list of directories.
2. For a computer running Microsoft Windows, in which directories can users **only read** files, but cannot write files? Document all the steps you take, do not only present a list of directories.
3. Which user-writable directories contain **executable files**? Executable files for the purpose of this question are those with an extension of bat, dll, exe, msi.
4. Which user-readable directories (that are not also user-writable) contain executable files?
5. What **specific directories** (and subdirectories) should be allowed in a path-based application whitelist based on your discoveries? Why?

Answers must be submitted in Moodle as PDF files following the naming convention:
Exercise02-YourLastName-YourFirstName.pdf
Example: Exercise02-Mustermann-Erika.pdf