EV3. Part 1. SQL Query Design

Assessable Task 3

Database Management (DBM)
NSM/ASIR

Pau Miñana
2023-2024

To Consider

This activity is optional but evaluative: it may affect your evaluation grade.

> 🚫 **If you look for solutions on the internet or ask the ChatGPT oracle, you will only be fooling yourself**. Remember that ChatGPT is not infallible or omnipotent. It is a great tool for speeding up your work once you have mastered a subject, but using it as a shortcut when you are acquiring basic skills and knowledge is seriously detrimental to your learning.
>
> Try to solve the activities using the resources we have seen and the extended documentation you will find in the Virtual Classroom.

INDEX

1. Instructions and rules

1.1. Description

You are required to de (MySQL) models that match the given specifications.

1.2. Delivery deadline and rates

- **EVALUATION ratio**: 30% of the total grade is for the assessable tasks.
- **ACTIVITY ratio**: 50% of the assessable tasks grade (there are two per evaluation).
- **DEADLINE**: *23:59 on Wednesday 27th March 2024* (6 WEEKS).

1.3. Grading

Submission is not compulsory and there is no minimum mark. **It will be graded from 0 to 10 according to the rating section** provided in this document.

1.4. Resources

You should study and consult all the resources given on the virtual classroom, paying particular attention to the non-assessable tasks and all the extra material.

To facilitate the correction of the activity use the provided template.

1.5. Plagiarism

You should avoid other students copying your work and take care to prevent this situation.

This is an **individual assignment**. If authorship is suspected, an oral interview will be required.

1.6. Submission instructions

Lhe assignment must be submitted as **a single PDF** containing the exercises solved according to the template.

ANY OTHER FORMAT WILL NOT BE ACCEPTED

1.7. Solutions and grading results

You will receive the grade broken down by section, and the overall score, along with any comments that provide suggestions on how you could improve.

2. Procedure to follow

1. Download the template and the script from the Virtual Classroom.
2. The physical schema is available in this document, although you can generate it with MySQL Workbench by following the steps in this video: https://www.youtube.com/watch?v=8M1eGDkWffk
3. **Remember that you need to work with this database, regardless of the diagram you presented in the previous assessable activity**.
4. Recommendations:
    1. It is advisable to design the queries on paper first and then test them in the DBMS itself. Remember that Ordinary and Extraordinary exams will be on paper. In addition, for technical reasons, the continuous assessment exam may also be paper based.
    2. Preferably use standard SQL. If you are using any functionality that is exclusive to MySQL, justify it every time time.
    3. Ensure that your query returns the requested data in the specified order and format.
    4. Use ALIAS where appropriate, case sensitivity, spaces and line breaks to make SQL as readable as possible.

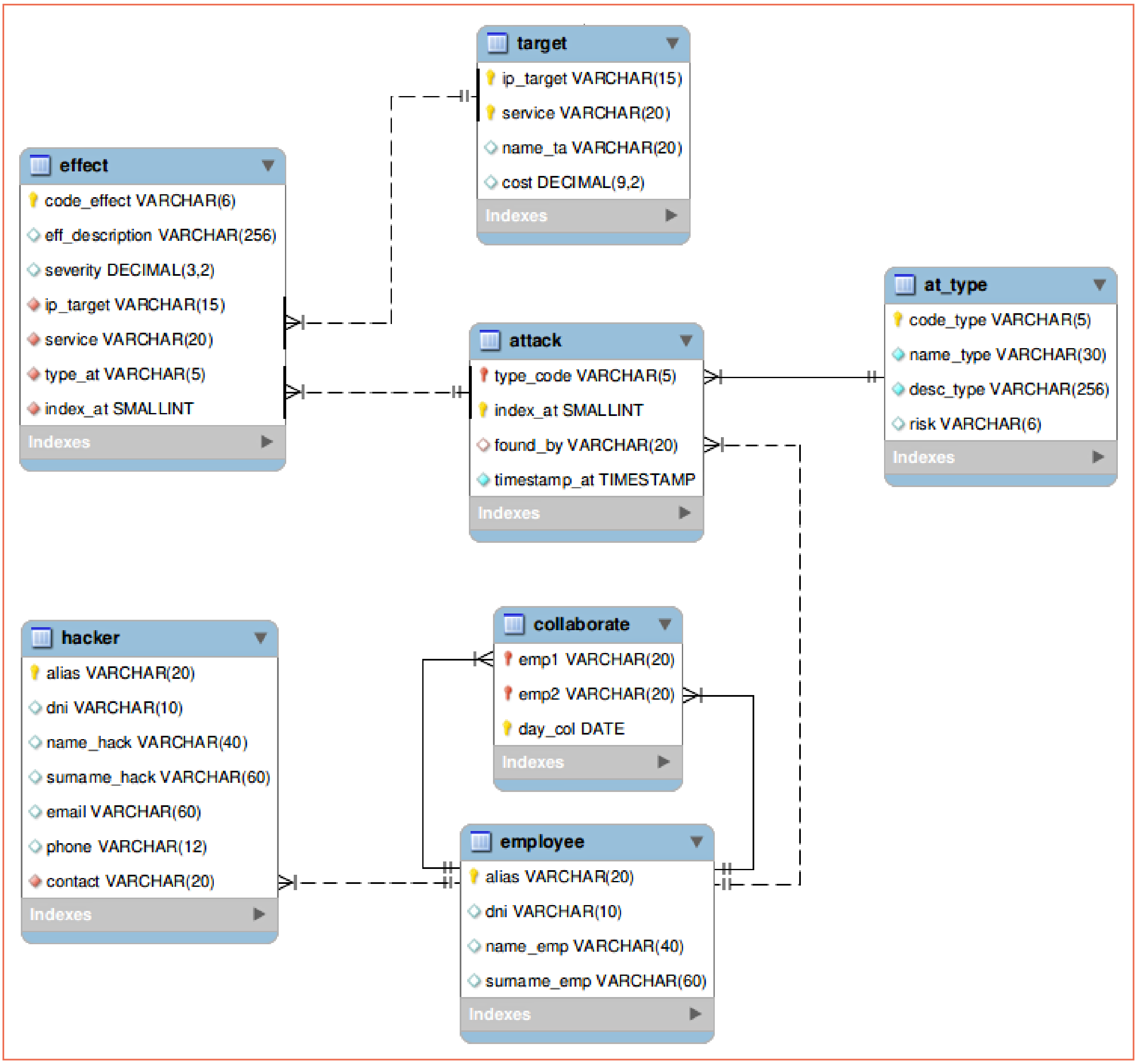
3. Rating

SECTION	RATING	SECTION	RATING
Query 1	1.25	Query 4	1.5
Query 2	1.25	Query 5	2
Query 3	1. 5	Query and View 6	2.5

GRADING CRITERIA

- The query returns the requested data in the specified order and format.
- Uses ALIAS where appropriate to make the query and response easier and clearer, makes appropriate use of case, spaces and line breaks to make SQL as readable as possible.
- Uses standard SQL syntax.
- Justifies and explains the use of MySQL syntax and elements.

4. Statement. Cyber Security Division (ASSESSABLE)



4.1. Query 1

Show the attacks found by employees working with hacker whose alias starts with the letter C, the alias of the hacker and a field with the full name of the employee with their alias in this format: name surname, "alias". Sort the result alphabetically by that field, type_code and at_type. Use the following methods:

a) Explicit nomenclature
b) Implicit nomenclature

4.2. Query 2

Show the name of the target and the average severity of all effects caused by attacks on that target, only if the average is greater than 60%. Sort the result from highest to lowest average severity.

Be careful, there are targets that share the same name. Use the following methods:

a) With GROUP BY
b) With subqueries

4.3. Query 3

Display the aliases of employees who have never worked with another employee, sorted by the last name of the employee. Use the following methods:

a) With IN
b) With EXISTS

4.3. Query 4

Show the attacks, their timestamps, and the first and last name of their finders (if any) of all attacks of the same type as the most recent attack, except this one. Sort the results by surname and from most recent to oldest.

4.5. Query 5

List how many attacks has received each target and sort the targets from least to most attacked. Be careful, the number of attacks is not the number of effects.

Now list the average number of attacks suffered by targets according to their service.

If you are unable to resolve it with the number of attacks, use the number of effects (for a maximum score of 1.5)

4.6. Query and view

Create a view that calculates the number of attacks found for each employee working with a hacker whose dni is unknown. The view will show the alias of the employee, the alias of the hacker and the number of attacks.

Show which employee(s) has/have found the most and how many attacks that meet the above conditions, first using the view and then without it.