Advanced Databases Assignment: Part

Database security project

Group Work

Due date: 06/09/2024
Presentation dates to be scheduled

Objective

To explore and apply practical database security measures using a combination of automated tools, scripting, and best practices. This assignment is divided into research-based tasks and hands-on activities that focus on critical aspects of database security.

Part 1: Database intruders

Research and report on the types of intruders that pose a threat to database systems. Include:
Insiders: Describe insider threats (e.g., disgruntled employees, privileged users, etc.) and how they compromise database security.

Outsiders: Describe outsider threats (e.g., hackers, cybercriminals) and their methods for exploiting database vulnerabilities.

Who Are We Securing Ourselves Against? How they attack databases?

- Identify and demonstrate at least two intruding tools,
- Technology used,
- how does it work,
- installation requirements,
- Defense techniques and tools

Part 2: Security on database installation (SQL Server, MySQL, Oracle)

Investigate security best practices during the installation and configuration of database management systems. Choose one of the following DBMSs: SQL Server, MySQL, and Oracle

For your chosen DBMS:

- Brief description of DBMS
- Editions and features
- Detail secure installation practices (e.g., permissions, configuration of network access).
- Provide a step-by-step guide to properly secure a fresh installation, highlighting key security settings.
- Installation requirements and pre-requisites software tools
- Database security measures before during and after installation

Part 3: Database security Testing – DBMS specific

- **Case 1: Database security testing**

Find and demonstrate one automated tool that aids in database security testing. Find and demonstrate one automated tool that aids in database security testing.

Write the report that will include:

- An overview of the tool's capabilities and how it works,
- A demonstration of its use on a test database,
- A summary of the vulnerabilities detected.

- **Case 2: Passive Reconnaissance Tools**

Find and describe at least two automated tools that can be used for passive reconnaissance.

Your report should:

- Provide an overview of each tool,
- Describe how these tools can be used to gather information about a database server without directly interacting with it.
- Give real-world examples of how passive reconnaissance is used in attacks.

- **Case 3: Active Reconnaissance Tools**

Find and demonstrate at least two automated tools that can be used for active reconnaissance.

Your report should Include:

- A detailed description of each tool's capabilities.
- Demonstration their usage by probing a test database environment.
- Discussion on how these tools could expose database vulnerabilities.

- **Case 4: Capturing Passwords**

Find and describe at least one automated tool for capturing and decrypting passwords within a database. (Additionally, provide a basic SQL script for simulating password encryption and decryption.)

Your report should include:

- A description of the tool and how it works.
- A demonstration of password capturing in a secure testing environment.
- An explanation of the SQL script and how encryption/decryption is managed in databases.

Part 4: Database maintenance (with scripting samples)

Research and demonstrate proper database maintenance practices with a focus on security.

- Define authentication and then implement with SQL Server, MySQL, and Oracle
- Define authorization and then implement with SQL Server, MySQL, and Oracle
- Manage users based on security best practices using SQL Server, MySQL, and Oracle
- Identify and apply password best practices using SQL Server, MySQL, and Oracle
- Define and create roles using SQL Server, MySQL, and Oracle
- Define, grant, deny, and revoke privileges using SQL Server, MySQL, and Oracle
- Define Automated backups using SQL Server, MySQL, and Oracle
- Define Database patch management using SQL Server, MySQL, and Oracle

Part 5: References

Include a well-formatted references section at the end of your report. Follow these guidelines:

- Format: Use either APA, IEEE, or Harvard referencing style. Sources: Cite all research papers, articles, software documentation, and tools used in your assignment.
- Ensure that you properly attribute every source you consulted during your research.
- Make sure that all in-text citations directly correspond to a complete entry in your References section.
- Failing to properly attribute sources can result in plagiarism, so ensure that your referencing is thorough and accurate.