

Poster

Try Hack Me



What is rdbms?

[Start Machine](#)

Depending on the EF Codd relational model, an RDBMS allows users to build, update, manage, and interact with a relational database, which stores data as a table.

Today, several companies use relational databases instead of flat files or hierarchical databases to store business data. This is because a relational database can handle a wide range of data formats and process queries efficiently. In addition, it organizes data into tables that can be linked internally based on common data. This allows the user to easily retrieve one or more tables with a single query. On the other hand, a flat file stores data in a single table structure, making it less efficient and consuming more space and memory.

Most commercially available RDBMSs currently use Structured Query Language (SQL) to access the database. RDBMS structures are most commonly used to perform CRUD operations (create, read, update, and delete), which are critical to support consistent data management.

Are you able to complete the challenge?

The machine may take up to 5 minutes to boot and configure

Answer the questions below

What is the rdbms installed on the server?

postgresql

Correct Answer

What port is the rdbms running on?

5432

Correct Answer

Metasploit contains a variety of modules that can be used to enumerate in multiple rdbms, making it easy to gather valuable information.

No answer needed

Correct Answer

After starting Metasploit, search for an associated auxiliary module that allows us to enumerate user credentials. What is the full path of the modules (starting with auxiliary)?

auxiliary/scanner/postgres/postgres_login

Correct Answer

What are the credentials you found?

example: user:password

postgres:password

Correct Answer

What is the full path of the module that allows you to execute commands with the proper user credentials (starting with auxiliary)?

auxiliary/admin/postgres/postgres_sql

Correct Answer

Based on the results of #6, what is the rdbms version installed on the server?

9.5.21

Correct Answer

What is the full path of the module that allows for dumping user hashes (starting with auxiliary)?

auxiliary/scanner/postgres/postgres_hashdump

Correct Answer

How many user hashes does the module dump?

6

Correct Answer

What is the full path of the module (starting with auxiliary) that allows an authenticated user to view files of their choosing on the server?

auxiliary/admin/postgres/postgres_readfile

Correct Answer

What is the full path of the module that allows arbitrary command execution with the proper user credentials (starting with exploit)?

exploit/multi/postgres/postgres_copy_from_program_cmd_exec

Correct Answer

What is the full path of the module that allows arbitrary command execution with the proper user credentials (starting with exploit)?

exploit/multi/postgres/postgres_copy_from_program_cmd_exec

Correct Answer

Compromise the machine and locate user.txt

THM{postgresql_fa1l_conf1guration}

Correct Answer

Hint

Escalate privileges and obtain root.txt

THM{c0ngrats_for_read_the_file_w1th_credent1als}

Correct Answer

