Another Hidden Page?!

CTFd	☑
Created	@June 15, 2021 11:07 AM
Done	☑
Hint	
author	Keita Togawa
field	Network
placement	placed
progress	Completed
value(50-200)	100
writeup	☐

概要

ラズパイ上で80番とは別のポートでWebサーバを立てておき，そっちを見に行けばFlagがとれる

`nmap`でポートスキャンしてもらって，`curl`で取りに行く

nmapはもともと入ってないので，aptの使いかたを別の問題で作ったほうがいいかも→作った

問題文

どうやらラズパイではWebサーバが起動しているらしい．ただ，httpのWellknownポートにアクセスしても・・・

Hint

もしあれば

問題ファイル

↓ `/etc/nginx/sites-enabled/default`

```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        root /var/www/html;

        index index.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }
}
server {
        listen 8000 default_server;
        listen [::]:8000 default_server;

        root /var/www/htp;

        index flag.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }
}
```

↓ `/var/www/html/index.html`

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
    body {
        width: 35em;
        margin: 0 auto;
        font-family: Tahoma, Verdana, Arial, sans-serif;
    }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
```

```
<!-- htp-ctf{TRUTH_IS_NOT_ONLY_VISIBLE} -->
<h1>This page is opened at 80/http</h1>
</body>
</html>
```

↓ `/var/www/htp/flag.html`

```
<!DOCTYPE html>
<html>
  <head>
    <title>ANOTHER WEB PAGE</title>
  </head>
  <body>
    <h1>You are greate Hacker! Flag is</h1>
    <h1>htp-ctf{WEB_IS_NOT_ONLY_80}</h1>
  </body>
</html>
```

```
## 問題の置き方
# 各ファイルを配置
sudo vim /etc/nginx/sites-enabled/default
sudo mkdir /var/www/htp
sudo vim /var/www/htp/flag.html

# 一般ユーザがファイルを直接見えないようにする
sudo chown -R root:www-data /var/www/htp/flag.html
sudo chmod 640 /var/www/htp/flag.html

# nginx restart
sudo systemctl restart nginx
```

Flag

これを入れるとAcceptする文字列

`htp-ctf{WEB_IS_NOT_ONLY_80}`

解法ざっくり

`nmap`して，開いてるポートを調べる

```
$ nmap localhost
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-22 07:18 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00046s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
```

```
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

ブラウザかcurlで，8000番を見に行く．